WILLIAM STALLINGS

EFFECTIVE CYBERSECURITY

A Guide to Using Best Practices and Standards



https://t.me/learningnets

Effective Cybersecurity

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Effective Cybersecurity

Understanding and Using Standards and Best Practices

William Stallings

Addison-Wesley

Upper Saddle River, NJ • Boston • San Francisco • New York
Toronto • Montreal • London • Munich • Paris • Madrid
Cape Town • Sydney • Tokyo • Singapore • Mexico City

https://t.me/learningnets

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2018941168

Copyright © 2019 Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearsoned.com/permissions/.

ISBN-13: 978-0-13-477280-6
ISBN-10: 0-13-477280-6

1 18

Executive Editor
Brett Bartow

Development Editor
Marianne Bartow

Managing Editor
Sandra Schroeder

Senior Project Editor
Lori Lyons

Copy Editor
Kitty Wilson

Project Manager
Dhayanidhi Karunanidhi

Indexer
Ken Johnson

Proofreader
Jeanine Furino

Technical Reviewers
Akhil Behl
Michael Shannon

Cover Designer
Chuti Praertsith

Compositor
codemantra

https://t.me/learningnets

To Tricia, my loving wife,
the kindest and gentlest person.

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Contents at a Glance

Preface xxvii

CHAPTER 1 Best Practices, Standards, and a Plan of Action. 2

PART I PLANNING FOR CYBERSECURITY 41

CHAPTER 2 Security Governance 42

CHAPTER 3 Information Risk Assessment 74

CHAPTER 4 Security Management 136

PART II MANAGING THE CYBERSECURITY FUNCTION 157

CHAPTER 5 People Management 160

CHAPTER 6 Information Management 178

CHAPTER 7 Physical Asset Management. 210

CHAPTER 8 System Development. 248

CHAPTER 9 Business Application Management 280

CHAPTER 10 System Access. 304

CHAPTER 11 System Management. 366

CHAPTER 12 Networks and Communications 392

CHAPTER 13 Supply Chain Management and Cloud Security 448

CHAPTER 14 Technical Security Management. 482

CHAPTER 15 Threat and Incident Management. 546

CHAPTER 16 Local Environment Management 602

CHAPTER 17 Business Continuity 622

https://t.me/learningnets

PART III SECURITY ASSESSMENT **665**

CHAPTER 18 Security Monitoring and Improvement 666

Appendix A: References and Standards 694

Appendix B: Glossary 708

Index 726

Appendix C (Online Only): Answers to Review Questions

You can find Appendix C at informit.com/title/9780134772806.
Click the Downloads tab to access the PDF file.

https://t.me/learningnets

Table of Contents

Preface xxvii

Chapter 1: Best Practices, Standards, and a Plan of Action 2

1.1 Defining Cyberspace and Cybersecurity 3

1.2 The Value of Standards and Best Practices Documents 6

1.3 The Standard of Good Practice for Information Security 7

1.4 The ISO/IEC 27000 Suite of Information Security Standards 12

ISO 27001 15

ISO 27002 17

1.5 Mapping the ISO 27000 Series to the ISF SGP 18

1.6 NIST Cybersecurity Framework and Security Documents 21

NIST Cybersecurity Framework 22

NIST Security Documents 25

1.7 The CIS Critical Security Controls for Effective Cyber Defense 27

1.8 COBIT 5 for Information Security 29

1.9 Payment Card Industry Data Security Standard (PCI DSS) 30

1.10 ITU-T Security Documents 32

1.11 Effective Cybersecurity 34

The Cybersecurity Management Process 34

Using Best Practices and Standards Documents 36

1.12 Key Terms and Review Questions 38

Key Terms 38

Review Questions 38

1.13 References 39

https://t.me/learningnets

Part I: Planning for Cybersecurity 41

Chapter 2: Security Governance 42

2.1 Security Governance and Security Management 43

2.2 Security Governance Principles and Desired Outcomes 45

Principles 45

Desired Outcomes. 46

2.3 Security Governance Components. 47

Strategic Planning 47

Organizational Structure 51

Roles and Responsibilities 55

Integration with Enterprise Architecture 58

Policies and Guidance 63

2.4 Security Governance Approach 63

Security Governance Framework. 63

Security Direction 64

Responsible, Accountable, Consulted, and Informed (RACI) Charts. 66

2.5 Security Governance Evaluation. 68

2.6 Security Governance Best Practices 69

2.7 Key Terms and Review Questions 70

Key Terms 70

Review Questions 71

2.8 References 71

Chapter 3: Information Risk Assessment 74

3.1 Risk Assessment Concepts. 75

Risk Assessment Challenges 78

Risk Management 80

Structure of This Chapter 84

https://t.me/learningnets

3.2 Asset Identification 85
Hardware Assets 85
Software Assets 85
Information Assets 86
Business Assets 87
Asset Register 87
3.3 Threat Identification 89
The STRIDE Threat Model 89
Threat Types 90
Sources of Information 92
3.4 Control Identification 98
3.5 Vulnerability Identification 102
Vulnerability Categories 103
National Vulnerability Database and Common Vulnerability Scoring System 103
3.6 Risk Assessment Approaches 107
Quantitative Versus Qualitative Risk Assessment 107
Simple Risk Analysis Worksheet 113
Factor Analysis of Information Risk 114
3.7 Likelihood Assessment 116
Estimating Threat Event Frequency 118
Estimating Vulnerability 119
Loss Event Frequency 121
3.8 Impact Assessment 122
Estimating the Primary Loss 124
Estimating the Secondary Loss 125
Business Impact Reference Table 126
3.9 Risk Determination 128

https://t.me/learningnets

3.10 Risk Evaluation 128
3.11 Risk Treatment 129
Risk Reduction 130
Risk Retention 130
Risk Avoidance 130
Risk Transfer 131
3.12 Risk Assessment Best Practices 131
3.13 Key Terms and Review Questions 132
Key Terms 132
Review Questions 133
3.14 References 134
Chapter 4: Security Management **136**
4.1 The Security Management Function 137
Security Planning 140
Capital Planning 142
4.2 Security Policy 145
Security Policy Categories 146
Security Policy Document Content 147
Management Guidelines for Security Policies 151
Monitoring the Policy 151
4.3 Acceptable Use Policy 152
4.4 Security Management Best Practices 154
4.5 Key Terms and Review Questions 154
Key Terms 154
Review Questions 155
4.6 References 155

https://t.me/learningnets

PART II: Managing the Cybersecurity Function 157

Chapter 5: People Management 160

5.1 Human Resource Security 161

Security in the Hiring Process 162

During Employment 164

Termination of Employment 165

5.2 Security Awareness and Education 166

Security Awareness 168

Cybersecurity Essentials Program 173

Role-Based Training 173

Education and Certification 174

5.3 People Management Best Practices 175

5.4 Key Terms and Review Questions 176

Key Terms 176

Review Questions 176

5.5 References 177

Chapter 6: Information Management 178

6.1 Information Classification and Handling 179

Information Classification 179

Information Labeling 185

Information Handling 186

6.2 Privacy 186

Privacy Threats 189

Privacy Principles and Policies 191

Privacy Controls 196

https://t.me/learningnets

6.3 Document and Records Management 198
Document Management 200
Records Management 202
6.4 Sensitive Physical Information 204
6.5 Information Management Best Practices 205
6.6 Key Terms and Review Questions 206
Key Terms 206
Review Questions 207
6.7 References 208
Chapter 7: Physical Asset Management **210**
7.1 Hardware Life Cycle Management 211
Planning 213
Acquisition 214
Deployment 214
Management 215
Disposition 216
7.2 Office Equipment 217
Threats and Vulnerabilities 217
Security Controls 219
Equipment Disposal 222
7.3 Industrial Control Systems 223
Differences Between IT Systems and Industrial Control Systems 225
ICS Security 227
7.4 Mobile Device Security 231
Mobile Device Technology 233
Mobile Ecosystem 234
Vulnerabilities 236

https://t.me/learningnets

Mobile Device Security Strategy 238
Resources for Mobile Device Security 243
7.5 Physical Asset Management Best Practices 244
7.6 Key Terms and Review Questions 245
Key Terms 245
Review Questions 245
7.7 References 246
Chapter 8: System Development **248**
8.1 System Development Life Cycle 248
NIST SDLC Model 249
The SGP's SDLC Model 252
DevOps 254
8.2 Incorporating Security into the SDLC 259
Initiation Phase 260
Development/Acquisition Phase 264
Implementation/Assessment Phase 266
Operations and Maintenance Phase 270
Disposal Phase 272
8.3 System Development Management 273
System Development Methodology 274
System Development Environments 275
Quality Assurance 277
8.4 System Development Best Practices 278
8.5 Key Terms and Review Questions 278
Key Terms 278
Review Questions 279
8.6 References 279

https://t.me/learningnets

Chapter 9: Business Application Management **280**

9.1 Application Management Concepts 281

Application Life Cycle Management 281

Application Portfolio Management 283

Application Performance Management 285

9.2 Corporate Business Application Security 287

Business Application Register 287

Business Application Protection 288

Browser-Based Application Protection 289

9.3 End User-Developed Applications (EUDAs) 295

Benefits of EUDAs 296

Risks of EUDAs 296

EUDA Security Framework 297

9.4 Business Application Management Best Practices 300

9.5 Key Terms and Review Questions 301

Key Terms 301

Review Questions 302

9.6 References 302

Chapter 10: System Access **304**

10.1 System Access Concepts 304

Authorization 306

10.2 User Authentication 307

A Model for Electronic User Authentication 307

Means of Authentication 310

Multifactor Authentication 311

10.3 Password-Based Authentication 312

The Vulnerability of Passwords 313

The Use of Hashed Passwords 315

https://t.me/learningnets

Password Cracking of User-Chosen Passwords 317
Password File Access Control 319
Password Selection 320
10.4 Possession-Based Authentication 322
Memory Cards 322
Smart Cards 323
Electronic Identity Cards 325
One-Time Password Device 328
Threats to Possession-Based Authentication 329
Security Controls for Possession-Based Authentication 330
10.5 Biometric Authentication 330
Criteria for Biometric Characteristics 331
Physical Characteristics Used in Biometric Applications 332
Operation of a Biometric Authentication System 333
Biometric Accuracy 335
Threats to Biometric Authentication 337
Security Controls for Biometric Authentication 339
10.6 Risk Assessment for User Authentication 341
Authenticator Assurance Levels 341
Selecting an AAL 342
Choosing an Authentication Method 345
10.7 Access Control 347
Subjects, Objects, and Access Rights 348
Access Control Policies 349
Discretionary Access Control 350
Role-Based Access Control 351
Attribute-Based Access Control 353
Access Control Metrics 358

https://t.me/learningnets

10.8 Customer Access 360
Customer Access Arrangements 360
Customer Contracts 361
Customer Connections 361
Protecting Customer Data 361
10.9 System Access Best Practices 362
10.10 Key Terms and Review Questions 363
Key Terms 363
Review Questions 363
10.11 References 364
Chapter 11: System Management **366**
11.1 Server Configuration 368
Threats to Servers 368
Requirements for Server Security 368
11.2 Virtual Servers 370
Virtualization Alternatives 371
Virtualization Security Issues 374
Securing Virtualization Systems 376
11.3 Network Storage Systems 377
11.4 Service Level Agreements 379
Network Providers 379
Computer Security Incident Response Team 381
Cloud Service Providers 382
11.5 Performance and Capacity Management 383
11.6 Backup 384
11.7 Change Management 386
11.8 System Management Best Practices 389

https://t.me/learningnets

11.9 Key Terms and Review Questions 390
Key Terms 390
Review Questions 390
11.10 References 391
Chapter 12: Networks and Communications 392
12.1 Network Management Concepts 393
Network Management Functions 393
Network Management Systems 399
Network Management Architecture 402
12.2 Firewalls 404
Firewall Characteristics 404
Types of Firewalls 406
Next-Generation Firewalls 414
DMZ Networks 414
The Modern IT Perimeter 416
12.3 Virtual Private Networks and IP Security 417
Virtual Private Networks 417
IPsec 418
Firewall-Based VPNs 420
12.4 Security Considerations for Network Management 421
Network Device Configuration 421
Physical Network Management 423
Wireless Access 426
External Network Connections 427
Firewalls 428
Remote Maintenance 429

https://t.me/learningnets

12.5 Electronic Communications 430
Email 430
Instant Messaging 436
Voice over IP (VoIP) Networks 438
Telephony and Conferencing 444
12.6 Networks and Communications Best Practices 444
12.7 Key Terms and Review Questions 445
Key Terms 445
Review Questions 445
12.8 References 446
Chapter 13: Supply Chain Management and Cloud Security 448
13.1 Supply Chain Management Concepts 449
The Supply Chain 449
Supply Chain Management 451
13.2 Supply Chain Risk Management 453
Supply Chain Threats 456
Supply Chain Vulnerabilities 459
Supply Chain Security Controls 460
SCRM Best Practices 463
13.3 Cloud Computing 466
Cloud Computing Elements 466
Cloud Computing Reference Architecture 470
13.4 Cloud Security 473
Security Considerations for Cloud Computing 473
Threats for Cloud Service Users 474
Risk Evaluation 475
Best Practices 476
Cloud Service Agreement 477

https://t.me/learningnets

13.5 Supply Chain Best Practices 478
13.6 Key Terms and Review Questions 479
Key Terms 479
Review Questions 479
13.7 References 480
Chapter 14: Technical Security Management **482**
14.1 Security Architecture 483
14.2 Malware Protection Activities 487
Types of Malware 487
The Nature of the Malware Threat 490
Practical Malware Protection 490
14.3 Malware Protection Software 494
Capabilities of Malware Protection Software 494
Managing Malware Protection Software 495
14.4 Identity and Access Management 496
IAM Architecture 497
Federated Identity Management 498
IAM Planning 500
IAM Best Practices 501
14.5 Intrusion Detection 502
Basic Principles 503
Approaches to Intrusion Detection 504
Host-Based Intrusion Detection Techniques 505
Network-Based Intrusion Detection Systems 506
IDS Best Practices 508
14.6 Data Loss Prevention 509
Data Classification and Identification 509
Data States 510

https://t.me/learningnets

14.7 Digital Rights Management 512
DRM Structure and Components 513
DRM Best Practices 515
14.8 Cryptographic Solutions 517
Uses of Cryptography 517
Cryptographic Algorithms 518
Selection of Cryptographic Algorithms and Lengths 525
Cryptography Implementation Considerations 526
14.9 Cryptographic Key Management 528
Key Types 530
Cryptoperiod 532
Key Life Cycle 534
14.10 Public Key Infrastructure 536
Public Key Certificates 536
PKI Architecture 538
Management Issues 540
14.11 Technical Security Management Best Practices 541
14.12 Key Terms and Review Questions 543
Key Terms 543
Review Questions 543
14.13 References 544
Chapter 15: Threat and Incident Management **546**
15.1 Technical Vulnerability Management 547
Plan Vulnerability Management 547
Discover Known Vulnerabilities 548
Scan for Vulnerabilities 549
Log and Report 551
Remediate Vulnerabilities 551

https://t.me/learningnets

15.2 Security Event Logging 554
Security Event Logging Objective 556
Potential Security Log Sources 556
What to Log 557
Protection of Log Data 557
Log Management Policy 558
15.3 Security Event Management 559
SEM Functions 560
SEM Best Practices 561
15.4 Threat Intelligence 563
Threat Taxonomy 564
The Importance of Threat Intelligence 566
Gathering Threat Intelligence 568
Threat Analysis 569
15.5 Cyber Attack Protection 570
Cyber Attack Kill Chain 570
Protection and Response Measures 573
Non-Malware Attacks 576
15.6 Security Incident Management Framework 577
Objectives of Incident Management 579
Relationship to Information Security Management System 579
Incident Management Policy 580
Roles and Responsibilities 581
Incident Management Information 583
Incident Management Tools 583
15.7 Security Incident Management Process 584
Preparing for Incident Response 585
Detection and Analysis 586

https://t.me/learningnets

Containment, Eradication, and Recovery 587
Post-Incident Activity 588
15.8 Emergency Fixes 590
15.9 Forensic Investigations 592
Prepare 593
Identify 594
Collect 594
Preserve 595
Analyze 595
Report 596
15.10 Threat and Incident Management Best Practices 597
15.11 Key Terms and Review Questions 598
Key Terms 598
Review Questions 599
15.12 References 599
Chapter 16: Local Environment Management **602**
16.1 Local Environment Security 602
Local Environment Profile 603
Local Security Coordination 604
16.2 Physical Security 606
Physical Security Threats 606
Physical Security Officer 609
Defense in Depth 610
Physical Security: Prevention and Mitigation Measures 612
Physical Security Controls 615
16.3 Local Environment Management Best Practices 619

https://t.me/learningnets

16.4 Key Terms and Review Questions 620
Key Terms 620
Review Questions 620
16.5 References 621
Chapter 17: Business Continuity **622**
17.1 Business Continuity Concepts 625
Threats 626
Business Continuity in Operation 628
Business Continuity Objectives 629
Essential Components for Maintaining Business Continuity 630
17.2 Business Continuity Program 630
Governance 631
Business Impact Analysis 631
Risk Assessment 632
Business Continuity Strategy 634
17.3 Business Continuity Readiness 637
Awareness 637
Training 638
Resilience 639
Control Selection 640
Business Continuity Plan 642
Exercising and Testing 647
Performance Evaluation 650
17.4 Business Continuity Operations 655
Emergency Response 655
Crisis Management 656
Business Recovery/Restoration 657

https://t.me/learningnets

17.5 Business Continuity Best Practices 660
17.6 Key Terms and Review Questions 661
Key Terms 661
Review Questions 661
17.7 References 662

Part III: Security Assessment **665**

Chapter 18: Security Monitoring and Improvement **666**

18.1 Security Audit 666
Security Audit and Alarms Model 667
Data to Collect for Auditing 668
Internal and External Audit 672
Security Audit Controls 673
18.2 Security Performance 678
Security Performance Measurement 678
Security Monitoring and Reporting 686
Information Risk Reporting 688
Information Security Compliance Monitoring 690
18.3 Security Monitoring and Improvement Best Practices 691
18.4 Key Terms and Review Questions 692
Key Terms 692
Review Questions 692
18.5 References 693

Appendix A: References and Standards **694**

Appendix B: Glossary **708**

Index **726**

Appendix C (Online Only): Answers to Review Questions

You can find Appendix C at informit.com/title/9780134772806.
Click the Downloads tab to access the PDF file.

https://t.me/learningnets

Preface

There is the book, Inspector. I leave it with you, and you cannot doubt that it contains a full explanation.

—*The Adventure of the Lion's Mane*, by Sir Arthur Conan Doyle

Background

Effective cybersecurity is very difficult. A number of organizations, based on wide professional input, have developed best-practices types of documents as well as standards for implementing and evaluating cybersecurity. On the standards side, the most prominent player is the National Institute of Standards and Technology (NIST). NIST has created a huge number of security publications, including 9 Federal Information Processing Standards (FIPS) and well over 100 active Special Publications (SP) that provide guidance on virtually all aspects of cybersecurity. Equally important is the International Organization for Standardization (ISO) 27000 series of standards on information security management systems. Other organizations that have produced cybersecurity standards and guidelines include:

- **ISACA/COBIT:** The COBIT-5 for information security and related documents are widely used by the industry.
- **ITU Telecommunication Standardization Sector (ITU-T):** Most important are the series X.1050 through X.1069 on security management.
- **Internet Society (ISOC):** A number of published standards and RFCs relate to cybersecurity.

In addition, a number of professional and industry groups have produced best-practices documents and guidelines. The most important such document is *The Standard of Good Practice for Information Security* (SGP), produced by the Information Security Forum (ISF). This almost 300-page document provides a wide range of best practices based on the consensus of industry and government organizations. Another key organization is the Center for Internet Security (CIS), which has published detailed lists of industry-approved security controls and metrics. Other respected organizations have also produced a number of similar documents.

Thus, there is an immense amount of practical, widely accepted material available. The problem is that the amount of information is so massive that it is difficult for cybersecurity practitioners to take advantage of it to build and maintain effective cybersecurity systems and policies.

The objective of this book is to organize, consolidate, and explain all this material to enable the security practitioner to make effective use of it.

This book is addressed to people in both IT and security management, people tasked with maintaining IT security, and a wide range of others interested in cybersecurity and information security.

https://t.me/learningnets

Organization of the Book

The book consists of three parts:

- **Part I, "Planning for Cybersecurity":** This part of the book provides guidelines for effectively managing the cybersecurity mission, including security governance and security requirements. The ISF defines *security governance* as "the framework by which policy and direction is set, providing senior management with assurance that security management activities are being performed correctly and consistently." Part I of this book provides guidance in developing a set of risk and security requirements to ensure that there are no gaps in an organization's cybersecurity practices.
- **Part II, "Managing the Cybersecurity Function":** This part of the book examines in detail the security controls intended to satisfy the defined security requirements. The 13 chapters in this part encompass the broad range of management, operational, and technical means used to achieve effective cybersecurity.
- **Part III, "Security Assessment":** This part of the book discusses techniques for auditing and monitoring the performance of cybersecurity controls, with a view to spotting gaps in the system and devising improvements.

Supporting Websites

The author maintains a companion website at WilliamStallings.com/Cybersecurity that includes a list of relevant links organized by chapter and an errata sheet for the book.



WilliamStallings.com/Cybersecurity
Companion website

The author also maintains the Computer Science Student Resource Site at ComputerScienceStudent.com. The purpose of this site is to provide documents, information, and links for computer science students and professionals. Links and documents are organized into seven categories:

- **Math:** Includes a basic math refresher, a queuing analysis primer, a number system primer, and links to numerous math sites.
- **How-to:** Provides advice and guidance for solving homework problems, writing technical reports, and preparing technical presentations.
- **Research resources:** Provides links to important collections of papers, technical reports, and bibliographies.
- **Other useful:** Provides a variety of other useful documents and links.
- **Computer science careers:** Lists useful links and documents for those considering a career in computer science.



ComputerScienceStudent.com
Computer Science Student
Resource Site

https://t.me/learningnets

- **Writing help:** Provides help in becoming a clearer, more effective writer.
- **Miscellaneous topics and humor:** You have to take your mind off your work once in a while.

Register This Book

Register your copy of *Effective Cybersecurity* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to informit.com/register and log in or create an account. Enter the product ISBN (9780134772806) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

Acknowledgments

This book has benefited from review by a number of people, who gave generously of their time and expertise. I especially thank Akhil Behl and Michael Shannon, who each devoted an enormous amount of time to a detailed review of the entire manuscript. I also thank the people who provided thoughtful reviews of the initial book proposal: Steven M. Bellovin, Kelley Dempsey, Charles A. Russell, Susan Sand, and Omar Santos.

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Sohail Awad, Vinay Banakar, Vilius Benetis, Rodrigo Ristow Branco, Michael Brown, Herve Carpentier, Jim Fenton, Adri Jovin, Joseph Kellegher, Adnan Kilic, Edward Lane, Junior Lazuardi, Matt Nichols, Omar Olivos, ShanShan Pa, Venkatesh Ramamoorthy, Antonius Ruslan, Jose Samuel, Jigar Savla, Matias Siri, and Dauda Sule. Nikhil Bhargava developed the review questions and answers.

Finally, I would like to thank the many people at Pearson responsible for the publication of the book. This includes the staff at Pearson, particularly Executive Editor Brett Bartow, Development Editor Marianne Bartow, and Senior Project Editor Lori Lyons. Thanks also to the marketing and sales staffs at Pearson, without whose efforts this book would not be in front of you.

With all this assistance, little remains for which I can take full credit. However, I am proud to say that, with no help whatsoever, I selected all the quotations.

About the Author and Contributors

Dr. William Stallings has made a unique contribution to understanding the broad sweep of technical developments in computer security, computer networking, and computer architecture. He has authored 18 textbooks, and, counting revised editions, a total of 70 books on various aspects of these subjects.

https://t.me/learningnets

His writings have appeared in numerous ACM and IEEE publications, including the *Proceedings of the IEEE* and *ACM Computing Reviews*. He has 13 times received the award for the best computer science textbook of the year from the Text and Academic Authors Association.

With more than 30 years in the field, he has been a technical contributor, a technical manager, and an executive with several high-technology firms. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. Currently, he is an independent consultant whose clients have included computer and networking manufacturers and customers, software development firms, and leading-edge government research institutions.

He created and maintains the Computer Science Student Resource Site at ComputerScienceStudent.com. This site provides documents and links on a variety of subjects of general interest to computer science students (and professionals). He is a member of the editorial board of *Cryptologia*, a scholarly journal devoted to all aspects of cryptology.

Dr. Stallings holds a Ph.D. from M.I.T. in computer science and a B.S. from Notre Dame in electrical engineering.

Technical Editors

Akhil Behl, CCIE No. 19564, is a passionate IT executive with a key focus on cloud and security. He has more than 15 years of experience in the IT industry, working in several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specialization includes cloud, security, infrastructure, data center, and business communication technologies.

Akhil is a published author. Over the past few years, Akhil has authored multiple titles on security and business communication technologies. He has contributed as a technical editor for more than a dozen books on security, networking, and information technology. He has published several research papers in national and international journals, including IEEE Xplore, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passions.

Akhil holds CCIE (Collaboration and Security), CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and a master's in business administration.

https://t.me/learningnets

Michael J. Shannon began his IT career when he transitioned from being a recording studio engineer to a network technician for a major telecommunications company in the early 1990s. He soon began to focus on security and was one of the first 10 people to attain the HIPAA Certified Security Specialist designation. Throughout his 30 years in IT, he has worked as an employee, a contractor, a trainer, and a consultant for a number of companies, including Platinum Technologies, Fujitsu, IBM, State Farm, Pearson, MindSharp, Thomson/NetG, and Skillsoft. Mr. Shannon has authored several books and training manuals, published articles, and produced dozens of CBT titles over the years as well. For security purposes, he has attained the CISSP, CCNP Security, SSCP, Security+, and ITIL Intermediate SO and RCV certifications. He is also a licensed insurance agent, specializing in cyber insurance on behalf of large insurers and numerous companies throughout Texas.

https://t.me/learningnets

Chapter 1

Best Practices, Standards, and a Plan of Action

There are some dogs who wouldn't debase what are to them sacred forms. A very fine, very serious German Shepherd I worked with, for instance, grumbled noisily at other dogs when they didn't obey. When training him to retrieve, at one point I set the dumbbell on its end for the fun of it. He glared disapprovingly at the dumbbell and at me, then pushed it carefully back into its proper position before picking it up and returning with it, rather sullenly.

—*Adam's Task: Calling Animals by Name*, Vicki Hearne

Learning Objectives

After studying this chapter, you should be able to:

- Explain the need for standards and best practices documents in cybersecurity.
- Present an overview of the Standard of Good Practice for Information Security.
- Explain the difference between ISO 27001 and ISO 27002.
- Discuss the role of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and how it differs from the objectives of ISO 27002.
- Explain the value of the Center for Internet Security (CIS) Critical Security Controls.

The purpose of this book is to provide security managers and security implementers with a comprehensive understanding of the technology, operational procedures, and management practices needed for effective cybersecurity. To that end, this book makes extensive use of standards and best practices documents that have broad support and are used to guide—and in many cases require—approaches to cybersecurity implementation. Although these documents represent the collective wisdom of numerous organizations and security experts, they are insufficient by themselves. These documents focus, mainly

https://t.me/learningnets

and in checklist fashion, on what needs to be done, but they do not provide tutorial material on the "how." With these considerations in mind, this book:

- Provides detailed explanations of the technology, operational procedures, and management practices needed to implement the guidelines and requirements of the standards and best practices documents. For example, a number of these documents call out the need for risk assessment but do not provide in-depth explanation or guidance of how to perform risk assessment. Chapter 3, "Information Risk Assessment," describes what is involved in performing a risk assessment.
- Provides a consolidated and comprehensive framework for implementing cybersecurity based on the many standards and best practices documents. This is not simply a summary or an outline of these documents. Rather, this book uses these documents to present a systematic and broad plan of action for implementing cybersecurity.

This chapter begins with a definition of cybersecurity and a discussion of the importance of standards and best practices documents in cybersecurity. The sections that follow look at the most significant sources of these documents for effective cybersecurity management. Finally, this chapter provides a discussion of the effective use of standards and best practices documents.

1.1 Defining Cyberspace and Cybersecurity

It is useful, at the start of the book, to have working definitions of *cyberspace* and *cybersecurity*. A useful definition of **cyberspace** comes from the National Research Council's publication *At the Nexus of Cybersecurity and Public Policy* [CLAR14]:

> **Cyberspace** consists of artifacts based on or dependent on computer and communications technology; the information that these artifacts use, store, handle, or process; and the interconnections among these various elements.

A reasonably comprehensive definition of **cybersecurity** is provided in ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.1205 [*Overview of Cybersecurity*, 2014]:

> **Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that are used to protect the cyberspace environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment. Cybersecurity strives to ensure the

https://t.me/learningnets

risk

A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.

asset

Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (that is, a system component, such as hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.

Two related terms should be mentioned:

- **Information security:** Preservation of confidentiality, integrity, and availability of information. In addition, other properties—such as authenticity, accountability, non-repudiation, and reliability—can also be involved.
- **Network security:** Protection of networks and their services from unauthorized modification, destruction, or disclosure and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects.

Cybersecurity encompasses information security, with respect to electronic information, and network security. Information security also is concerned with physical (for example, paper-based) information. However, in practice, the terms *cybersecurity* and *information security* are often used interchangeably.

Figure 1.1 illustrates essential cybersecurity objectives.

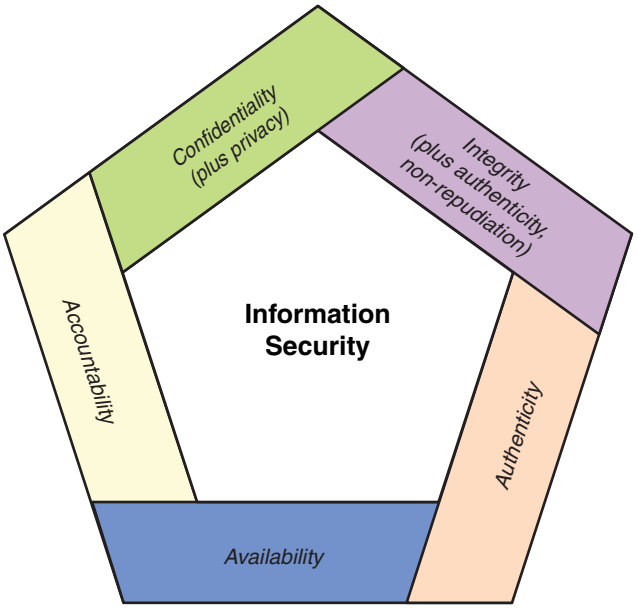


FIGURE 1.1 Essential Cybersecurity Objectives

https://t.me/learningnets

A more extensive list of cybersecurity objectives includes the following:

- **Availability:** The property of a system or a system resource being accessible or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; that is, a system is available if it provides services according to the system design whenever users request them.
- **Integrity:** The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
- **Authenticity:** The property of being genuine and being able to be verified and trusted. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Non-repudiation:** Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
- **Confidentiality:** The property that data is not disclosed to system entities unless they have been authorized to know the data.
- **Accountability:** The property of a system or system resource ensuring that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.

Cybersecurity Dilemmas: Technology, Policy, and Incentives [CICE14] summarizes the challenges in developing an effective cybersecurity system as follows:

- **Scale and complexity of cyberspace:** The scale and complexity of cyberspace are massive. Cyberspace involves mobile devices, workstations, servers, massive data centers, cloud computing services, Internet of Things (IoT) deployments, and a wide variety of wired and wireless networks. The variety of individuals and applications requiring some level of access to these resources is also huge. Further, the challenges to achieving cybersecurity constantly change as technologies advance, new applications of information technologies emerge, and societal norms evolve.
- **Nature of the threat:** Organizational assets in cyberspace are under constant and evolving **threat** from vandals, criminals, terrorists, hostile states, and other malevolent actors. In addition, a variety of legitimate actors, including businesses and governments, are interested in collecting, analyzing, and storing information from and about individuals and organizations, potentially creating security and privacy risks.

threat

A potential for violation of security that exists when there is a circumstance, a capability, an action, or an event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

vulnerability

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

https://t.me/learningnets

- **User needs versus security implementation:** Users want technology with the most modern and powerful features, that is convenient to use, that offers anonymity in certain circumstances, and that is secure. But there is an inherent conflict between greater ease of use and greater range of options on the one hand and robust security on the other. In general, the simpler the system, and the more its individual elements are isolated from one another, the easier it is to implement effective security. But over time, people demand more functionality, and the greater complexity that results makes systems less secure. Users or groups within an organization that feel inconvenienced by security mechanisms will be tempted to find ways around those mechanisms or demand relaxation of the security requirements.
- **Difficulty estimating costs and benefits:** It is difficult to estimate the total cost of cybersecurity breaches and, therefore, the benefits of security policies and mechanisms. This complicates the need to achieve consensus on the allocation of resources to security.

Because of these challenges, there is an ongoing effort to develop best practices, documents, and standards that provide guidance to managers charged with making resource allocation decisions as well as those charged with implementing an effective cybersecurity framework. The focus of this book is on the broad consensus that has been reached, as expressed in such documents. The volume and variety of these documents is very broad, and the goal of this book is to consolidate that material and make it accessible.

1.2 The Value of Standards and Best Practices Documents

The development, implementation, and management of a cybersecurity system for an organization are extraordinarily complex and difficult. A wide variety of technical approaches are involved, including cryptography, network security protocols, operating system mechanisms, database security schemes, and malware identification. The areas of concern are broad, including stored data, data communications, human factors, physical asset and property security, and legal, regulatory, and contractual concerns. And there is an ongoing need to maintain high confidence in the cybersecurity capability in the face of evolving IT systems, relationships with outside parties, personnel turnover, changes to the physical plant, and the ever-evolving threat landscape.

Effective cybersecurity is very difficult, and any attempt to develop an ad hoc, grow-your-own approach to cybersecurity is an invitation to failure. The good news is that a great deal of thought, experimentation, and implementation experience have

https://t.me/learningnets

already gone into the development of policies, procedures, and overall guidance for cybersecurity system management teams. A number of organizations, based on wide professional input, have developed best practices types of documents as well as standards for implementing and evaluating cybersecurity. On the standards side, the most prominent player is the National Institute of Standards and Technology (NIST). NIST has a huge number of security publications, including nine Federal Information Processing Standards (FIPS) and well 100 active Special Publications (SP) that provide guidance on virtually all aspects of cybersecurity. Other organization that have produced cybersecurity standards and guidelines include the ITU-T, International Organization for Standardization (ISO), and the Internet Society (ISOC).

In addition, a number of professional and industry groups have produced best practices documents and guidelines. The most important such document is the Standard of Good Practice for Information Security, produced by the Information Security Forum (ISF). This 300-plus-page document provides a wide range of best practices representing the consensus of industry and government organizations. Other respected organizations, including the Information Systems Audit and Control Association (ISACA) and the Payment Card Industry (PCI), have produced a number of similar documents.

Table 1.1 lists the most prominent best practices and standards documents that are discussed in this book.

TABLE 1.1 Important Best Practices and Standards Documents

Source	Title	Date
ISF	Standard of Good Practice for Information Security	2016
ISO	ISO 27002: Code of Practice for Information Security Controls	2013
NIST	Framework for Improving Critical Infrastructure Cybersecurity	2017
Center for Internet Security (CIS)	CIS Critical Security Controls for Effective Cyber Defense Version 7	2018
ISACA	COBIT 5 for Information Security	2012
PCI Security Standards Council	Data Security Standard v3.2: Requirements and Security Assessment Procedures	2016

1.3 The Standard of Good Practice for Information Security

The ISF is an independent, not-for-profit association of leading organizations from around the world. ISF members fund and cooperate in the development of a practical research program in information security. It is dedicated to investing, clarifying,

https://t.me/learningnets



Information Security Forum https://www.securityforum.org/tool/the-isf-standardrmation-security/

and resolving key issues in cybersecurity, information security, and risk management and to developing best practice methodologies, processes, and solutions that meet the business needs of its members. ISF members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organizations and developed through an extensive research and work program.

The most significant activity of the ISF is the ongoing development of the Standard of Good Practice for Information Security (SGP). This document is a business-focused, comprehensive guide to identifying and managing information security risks in organizations and their supply chains. The breadth of the consensus in developing the SGP is unmatched. The SGP is based on research projects and input from ISF members, as well as analysis of the leading standards on cybersecurity, information security, and risk management. In creating and updating the SGP, the goal of the ISF is the development of best practice methodologies, processes, and solutions that meet the needs of its members, including large and small business organizations, government agencies, and nonprofit organizations.

The SGP, first released in 1996, has gone through numerous revisions. The current version, as of this writing, is the 2016 version. The development of the standard is based on the results of four main groups of activities, shown in Figure 1.2.

- An extensive work program involving the expertise of a full-time ISF management team that performs comprehensive research into hot topics in information security; produces reports, tools, and methodologies; and maintains strategic projects such as the ISF's Information Risk Analysis Methodology (IRAM).
- Analysis and integration of information security–related standards (for example, ISO 27002, COBIT v5.1) and legal and regulatory requirements (for example, the Sarbanes-Oxley Act 2002, the PCI Data Security Standard, Basel II 1998, the EU Directive on Data Protection). All of the standards listed in Table 1.1 are incorporated into the SGP.
- The involvement of ISF members, using techniques such as workshops, face-to-face meetings, and interviews to contribute their practical experience.
- The results of the ISF Benchmark, which provide valuable insights into how information security is applied in member organizations.

https://t.me/learningnets

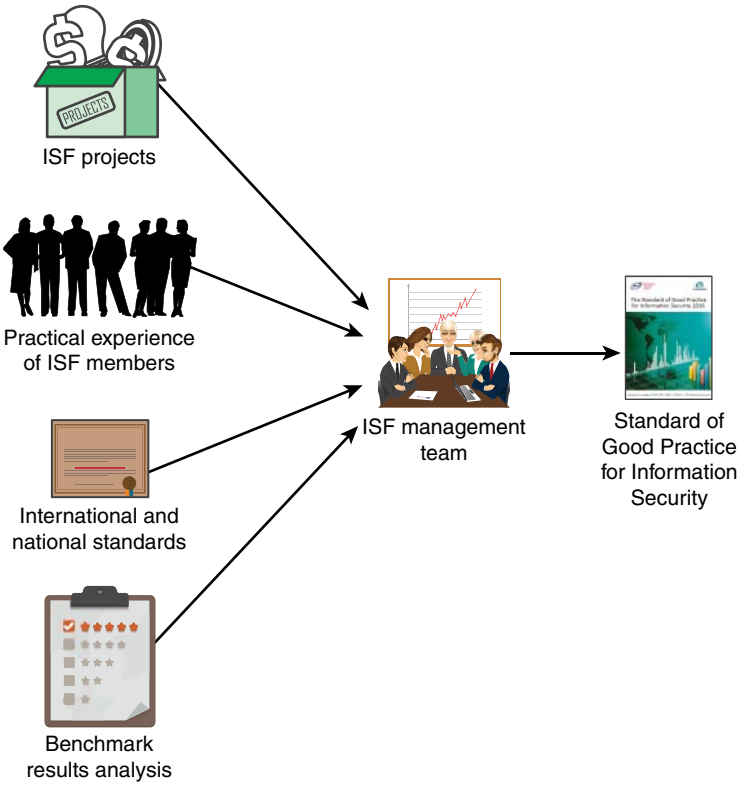


FIGURE 1.2 Basis for the ISF Standard of Good Practice for Information Security

The SGP is of particular interest to the following individuals:

- **Chief information security officers (or equivalent):** Responsible for developing policy and implementing sound information security governance and information security assurance.
- **Information security managers (as well as security architects, local security coordinators, and information protection champions):** Responsible for promoting or implementing an information security assurance program
- **Business managers:** Responsible for ensuring that critical business applications, processes, and local environments on which an organization's success depends are effectively managed and controlled
- **IT managers and technical staff:** Responsible for designing, planning, developing, deploying, and maintaining key business applications, information systems, or facilities

security policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

https://t.me/learningnets

- **Internal and external auditors:** Responsible for conducting security audits
- **IT service providers:** Responsible for managing critical facilities (for example, computer installations, networks) on behalf of the organization
- **Procurement and vendor management teams:** Responsible for defining appropriate information security requirements in contracts

The SGP is organized into 17 *categories*, each of which is broken down into 2 *areas* (see Table 1.2). Each area is further broken down into a number of *topics*, or business activities, for a total of 132 topics. Each of the 132 topics addresses good practice controls relevant to a particular activity from an information security perspective. Further, each topic is broken down into a number of subtopics, providing a substantial amount of detailed information and guidance. The SGP is consistent with the structure and flow of the ISO/IEC 27000 suite of standards (described in Section 1.4) and is suitable for organizations that want to use it in pursuing ISO compliance or certification or in implementing one or more information security management systems (ISMSs). The structure of the SGP reflects a broad consensus that has evolved and has been refined over more than 20 years, and the following 17 chapters of this book correspond to the 17 categories of the SGP. Thus, each chapter serves as a guide and source of background material on its respective category.

TABLE 1.2 ISF Standard of Good Practice for Information Security: Categories and Areas

Category	Areas
Security Governance (SG)	Security Governance Approach Security Governance Components
Information Risk Assessment (IR)	Information Risk Assessment Framework Information Risk Assessment Process
Security Management (SM)	Security Policy Management Information Security Management
People Management (PM)	Human Resource Security Security Awareness/Education
Information Management (IM)	Information Classification and Privacy Information Protection
Physical Asset Management (PA)	Equipment Management Mobile Computing
System Development (SD)	System Development Management System Development Life Cycle
Business Application Management (BA)	Corporate Business Applications End User Developed Applications

https://t.me/learningnets

Category	Areas
System Access (SA)	Access Management Customer Access
System Management (SY)	System Configuration System Maintenance
Networks and Communications (NC)	Network Management Electronic Communication
Supply Chain Management (SC)	External Supplier Management Cloud Computing
Technical Security Management (TS)	Security Solutions Cryptography
Threat and Incident Management (TM)	Cybersecurity Resilience Security Incident Management
Local Environment Management (LE)	Local Environments Physical and Environmental Security
Business Continuity (BC)	Business Continuity Framework Business Continuity Process
Security Monitoring and Improvement (SI)	Security Audit Security Performance

It is informative to consider the 17 SGP categories as being organized into three principal activities (see Figure 1.3):

1. **Planning for cybersecurity:** Developing approaches for managing and controlling the cybersecurity function(s); defining the requirements specific to a given IT environment; and developing policies and procedures for managing the security function
2. **Managing the cybersecurity function:** Deploying and managing the security controls to satisfy the defined security requirements
3. **Security assessment:** Assuring that the security management function enables business continuity; monitoring, assessing, and improving the suite of cybersecurity controls

The arrows in Figure 1.3 suggest that these activities occur an ongoing process. We return to this concept in Section 1.11.

https://t.me/learningnets

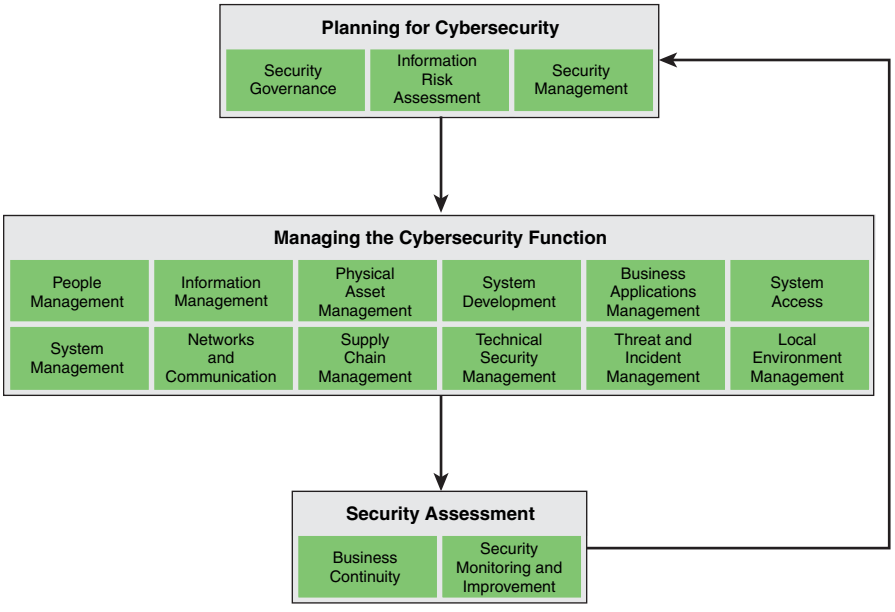


FIGURE 1.3 Categories in the Standard of Good Practice for Information Security

1.4 The ISO/IEC 27000 Suite of Information Security Standards



International Organization for Standardization https://www.iso.org/home.html

Perhaps the most important set of standards for cybersecurity is the ISO 27000 suite of information security standards. The ISO is an international agency for the development of standards on a wide range of subjects. It is a voluntary, nontreaty organization whose members are designated standards bodies of participating nations as well as nonvoting observer organizations. Although the ISO is not a government body, more than 70% of ISO member bodies are government standards institutions or organizations incorporated by public law. Most of the remainder have close links with the public administrations in their own countries. The U.S. member body is the American National Standards Institute (ANSI).

The ISO, which was founded in 1946, has issued more than 12,000 standards in a broad range of areas. Its purpose is to promote the development of standardization and related activities to facilitate international exchange of goods and services and to develop cooperation in the sphere of intellectual, scientific, technological, and economic activity. It has issued standards covering everything from screw threads to solar energy. One important area of ISO standardization deals with the Open Systems

https://t.me/learningnets

Interconnection (OSI) communications architecture and the standards at each layer of this architecture.

In the areas of data communications, networking, and security, ISO standards are developed in a joint effort with another standards body, the International Electrotechnical Commission (IEC). The IEC is primarily concerned with electrical and electronic engineering standards. The interests of the two groups overlap in the area of information technology, with the IEC emphasizing hardware and the ISO focusing on software. In 1987, the two groups formed the Joint Technical Committee 1 (JTC 1). This committee has the responsibility of developing the documents that ultimately become ISO (and IEC) standards in the area of information technology.

In the area of information security, together the ISO and IEC have developed a growing family of standards in the ISO/IEC 27000 series that deal with ISMSs.[1] The ISO 27000 definition of *ISMS* substantially addresses the concerns of this book:

> **Information security management system** consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analyzing requirements for the protection of assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:
>
> awareness of the need for information security
>
> assignment of responsibility for information security;
>
> incorporating management commitment and the interests of stakeholders
>
> enhancing societal values
>
> risk assessments determining appropriate controls to reach acceptable levels of risk
>
> security incorporated as an essential element of information networks and systems
>
> active prevention and detection of information security incidents
>
> ensuring a comprehensive approach to information security management
>
> continual reassessment of information security and making of modifications as appropriate

1. Throughout the rest of this book, for brevity, ISO/IEC standards are simply designated as ISO standards.

https://t.me/learningnets

The ISO 27000 series deals with all aspects of an ISMS. It helps small, medium, and large businesses in any sector keep information assets secure. This growing collection of standards falls into four categories (see Figure 1.4):

- **Overview and vocabulary:** Provide an overview and relevant vocabulary for ISMS
- **Requirements:** Discuss normative standards that define requirements for an ISMS and for those certifying such systems
- **Guidelines:** Provide direct support and detailed guidance and/or interpretation for the overall process of establishing, implementing, maintaining, and improving an ISMS
- **Sector-specific guidelines:** Address sector-specific guidelines for an ISMS

ISMS overview and vocabulary	ISMS requirements		ISMS guidelines		ISMS sector-specific guidelines	
27000 ISMS overview	27001 ISMS requirements	27006 Audit and certification of ISMS	27002 Code of practice for IS controls	27003 ISMS implementation	27010 Intersector/ interorganizational comms	27011 Telecomms organizations
	27009 Sector-specific application		27004 ISM measurement	27005 IS risk management	27015 Financial services	27017 IS controls for cloud services
			27007 ISMS auditing	TR 27008 Auditors on IS control	27018 Protection of PII in public clouds	27019 Energy utility industry PCS
			27013 Integrated implementation of 27001/20000	27014 Governance of IS		
			TR 27016 Organizational economics	27036 IS for supplier relationships		

ISMS = Information Security Management System
PII = personally identifiable information
PCS = process control systems

FIGURE 1.4 ISO 27000 ISMS Family of Standards

The most significant documents in the series are those that are cited in the ISF SGP:

- **ISO 27001: ISMS Requirements:** Provides a mandatory set of steps—such as defining a target environment, assessing risks, and selecting appropriate controls—for creating an ISMS, against which an organization can certify its security arrangements.
- **ISO 27002: Code of Practice for Information Security Controls:** Provides a framework of security controls that can be used to help select the controls required in an ISMS.

https://t.me/learningnets

- **ISO 27005: Information Security Risk Management System Implementation Guidance:** Provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk reporting, risk monitoring, and risk review. Examples of risk assessment methodologies are included as well.
- **ISO 27014: Governance of Information Security:** Provides guidance on principles and processes for the governance of information security, by which organizations can evaluate, direct, and monitor the management of information security.
- **ISO 27036: Information Security for Supplier Relationships:** Outlines information security for external parties for both the acquirers and suppliers. It supports organizations in implementing information **security controls** related to supplier relationships.

security controls

The management, operational, and technical controls (that is, countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

ISO 27001

Although ISO 27001 is brief, it is an important document for organizational executives with security responsibility. It is used to define the requirements for an ISMS in such a way that it serves as a checklist for certification. **Certification** gives credibility to an organization, demonstrating that a product or service meets the expectations of the organization's customers. For example, security certification using ISO 27001 is a way for executives to be assured that the security capability was funded and implemented and meets the security requirements of the organization. For some industries, certification is a legal or contractual requirement. A number of independent certification bodies provide certification services.

certification

The provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements. Also known as third-party conformity assessment.

According to an article in *ISSA Journal*, ISO 27001 certification confers the following benefits [LAMB06]:

- Certification assures an organization that it is following practices that broad experience has shown reduce the risk of security breaches.
- Certification assures an organization that it is following practices that broad experience has shown reduce the impact of any breach that does occur.
- If an organization can attest that its security and record handling procedures have been certified, this should reduce the potential penalty for a security breach imposed by regulators. The certification indicates a good faith effort to following broadly accepted best practices and standards.
- Certification assures stakeholders that the organization has developed and implemented sound security policy.
- Certification provides independent third-party validation of an organization's ISMS.
- Certification to the ISO 27001 standard is the most comprehensive information security standard that is internationally accepted.

https://t.me/learningnets

ISO 27001 is a management standard initially designed for the certification of organizations. The system works like this: An organization develops an ISMS, which consists of policies, procedures, people, technology, and so on, and then invites a certification body to determine that the ISMS is compliant with the standard; this is called a *certification audit*. Of course, there must be qualified individuals to develop and maintain the ISMS. Thus, various certification programs have been developed for individuals, the most common being for ISO 27001 Lead Implementer and ISO 27001 Lead Auditor programs. Obtaining such a certification enhances the value of an employee to an organization.

Table 1.3 lists the requirements and topics covered by ISO 27001 (using the numbering scheme in the ISO document).

TABLE 1.3 ISO 27001 Requirements Topics

Requirement	Topics
4 Context of the Organization	**4.1** Understanding the Organization and Its Context **4.2** Understanding the Needs and Expectations of Interested Parties **4.3** Determining the Scope of the Information Security Management System **4.4** Information Security Management System
5 Leadership	**5.1** Leadership and Commitment **5.2** Policy **5.3** Organizational Roles, Responsibilities and Authorities
6 Planning	**6.1** Actions to Address Risks and Opportunities **6.2** Information Security Objectives and Planning to Achieve Them
7 Support	**7.1** Resources **7.2** Competence **7.3** Awareness **7.4** Communication **7.5** Documented Information
8 Operation	**8.1** Operational Planning and Control **8.2** Information Security Risk Assessment **8.3** Information Security Risk Treatment
9 Performance Evaluation	**9.1** Monitoring, Measurement, Analysis and Evaluation **9.2** Internal Audit **9.3** Management Review
10 Improvement	**10.1** Nonconformity and Corrective Action **10.2** Continual Improvement

https://t.me/learningnets

ISO 27002

Although ISO 27001 lays out the requirements for an ISMS, it is rather general, and the specification of the requirements is only nine pages long. Of equal importance is ISO 27002, Code of Practice for Information Security Controls, which provides the broadest treatment of ISMS topics in the ISO 27000 series and comprises 90 pages. The linkage between the ISMS requirements defined in ISO 27001 and the information security controls defined in ISO 27002 is provided by Section 6.1.3 of ISO 27001, Information Security Risk Treatment. In essence, this section requires that an organization develop a risk treatment process by determining what controls must be implemented for the risk treatment options chosen. The section then references the controls in ISO 27002 and indicates that the organization can pick and choose the controls that are needed to satisfy the ISMS requirements. But ISO 27001 also states that the organization can select controls from any source, not solely or necessarily ISO 27002.

Table 1.4 lists the topics covered in ISO 27002 (using the numbering scheme in the ISO document). It should be mentioned that ISO 27001 and 27002 do not cover a number of important topics discussed in the ISF SGP, including threat intelligence and system decommissioning, and the ISF SGP is far more detailed, at 320 pages.

TABLE 1.4 ISO 27002 Control Topics

Control	Topics
5 Information Security Policies	**5.1** Management Direction for Information Security
6 Organization of Information Security	**6.1** Internal Organization **6.2** Mobile Devices and Teleworking
7 Human Resource Security	**7.1** Prior to Employment **7.2** During Employment **7.3** Termination and Change of Employment
8 Asset Management	**8.1** Responsibility for Assets **8.2** Information Classification **8.3** Media Handling
9 Access Control	**9.1** Business Requirements of Access Control **9.2** User Access Management **9.3** User Responsibilities **9.4** System and Application Access Control
10 Cryptography	**10.1** Cryptographic Controls
11 Physical and Environmental Security	**11.1** Secure Areas **11.2** Equipment
12 Operations Security	**12.1** Operational Procedures and Responsibilities **12.2** Protection from Malware **12.3** Backup **12.4** Logging and Monitoring **12.5** Control of Operational Software **12.6** Technical Vulnerability Management **12.7** Information Systems Audit Considerations

https://t.me/learningnets

Control	Topics
13 Communications Security	**13.1** Network Security Management **13.2** Information Transfer
14 System Acquisition, Development and Maintenance	**14.1** Security Requirements of Information Systems **14.2** Security in Development and Support Processes **14.3** Test Data
15 Supplier Relationships	**15.1** Information Security in Supplier Relationships
16 Information Security Incident Management	**16.1** Management of Information Security Incidents and Improvements
17 Information Security Aspects of Business Continuity Management	**17.1** Information Security Continuity **17.2** Redundancies
18 Compliance	**18.1** Compliance with Legal and Contractual Requirements **18.2** Information Security Reviews

1.5 Mapping the ISO 27000 Series to the ISF SGP

For an organization that relies on ISO 27001 for certification and ISO 27002 for a selection of controls to meet ISO 27001 requirements, the ISF SGP is an invaluable and perhaps essential tool. It provides a far more detailed description of the controls and represents the widest possible consensus among industry, government, and academic security experts and practitioners.

Table 1.5 shows maps the ISO 27001 requirements to the ISF SGP security controls. For each of the detailed requirements, this table indicates the controls that can be used to satisfy those requirements, as documented in the ISF SGP.

TABLE 1.5 Mapping ISO 27001 to the ISF SGP

ISO 27001 Topic	ISF SGP Category
4.1 Understanding the Organization and Its Context	Security Governance
4.2 Understanding the Needs and Expectations of Interested Parties	Security Governance
4.3 Determining the Scope of the Information Security Management System	Security Management
4.4 Information Security Management System	Security Management

https://t.me/learningnets

ISO 27001 Topic	ISF SGP Category
5.1 Leadership and Commitment	Security Governance
5.2 Policy	Security Management
5.3 Organizational Roles, Responsibilities and Authorities	Security Governance
6.1 Actions to Address Risks and Opportunities	Information Risk Assessment
6.2 Information Security Objectives and Planning to Achieve Them	Security Management
7.1 Resources	Security Management
7.2 Competence	People Management
7.3 Awareness	People Management
7.4 Communication	People Management
7.5 Documented Information	Security Management
8.1 Operational Planning and Control	Security Management
8.2 Information Security Risk Assessment	Information Risk Assessment
8.3 Information Security Risk Treatment	Information Risk Assessment
9.1 Monitoring, Measurement, Analysis and Evaluation	Security Monitoring and Improvement
9.2 Internal Audit	Security Monitoring and Improvement
9.3 Management Review	Security Monitoring and Improvement
10.1 Non-conformity and Corrective Action	Security Monitoring and Improvement
10.2 Continual Improvement	Security Monitoring and Improvement

Similarly, Table 1.6 shows the mapping between the ISO 27002 security controls and the corresponding controls in ISF SGP. Even if an organization is using ISO 27002 as a checklist of controls to be chosen to meet security requirements, these selections should be augmented by the more detailed information available in the ISF SGP.

TABLE 1.6 Mapping ISO 27002 to the ISF SGP

ISO 27002 Topic	ISF SGP Category
5.1 Management Direction for Information Security	Security Monitoring and Improvement
6.1 Internal Organization	Security Governance
6.2 Mobile Devices and Teleworking	People Management
7.1 Prior to Employment	People Management
7.2 During Employment	People Management
7.3 Termination and Change of Employment	People Management
8.1 Responsibility for Assets	Physical Asset Management
8.2 Information Classification	Physical Asset Management

https://t.me/learningnets

ISO 27002 Topic	ISF SGP Category
8.3 Media Handling	Physical Asset Management
9.1 Business Requirements of Access Control	System Access
9.2 User Access Management	System Access
9.3 User Responsibilities	System Access
9.4 System and Application Access Control	
10.1 Cryptographic Controls	Technical Security Management
11.1 Secure Areas	Local Environment Management
11.2 Equipment	Local Environment Management
12.1 Operational Procedures and Responsibilities	System Development
12.2 Protection from Malware	Technical Security Management
12.3 Backup	System Management
12.4 Logging and Monitoring	Threat and Incident Management
12.5 Control of Operational Software	XX
12.6 Technical Vulnerability Management	System Development
12.7 Information Systems Audit Considerations	Security Monitoring and Improvement
13.1 Network Security Management	Networks and Communications
13.2 Information Transfer	Networks and Communications
14.1 Security Requirements of Information Systems	Security Management
14.2 Security in Development and Support Processes	System Development
14.3 Test Data	System Development
15.1 Information Security in Supplier Relationships	Supply Chain Management
16.1 Management of Information Security Incidents and Improvements	Threat and Incident Management
17.1 Information Security Continuity	Business Continuity
17.2 Redundancies	Business Continuity
18.1 Compliance with Legal and Contractual Requirements	Security Management
18.2 Information Security Reviews	Security Monitoring and Improvement

As an example of the benefit of the ISF SGP, consider the category of threat and incident management. In ISO 27002, this category is defined in Section 16 in 4 pages and includes the following 7 subtopics:

- 16.1.1 Responsibilities and Procedures
- 16.1.2 Reporting Information Security Events

https://t.me/learningnets

- 16.1.3 Reporting Information Security Weaknesses
- 16.1.4 Assessment of and Decision on Information Security Events
- 16.1.5 Response to Information Security Incidents
- 16.1.6 Learning from Information Security Incidents
- 16.1.7 Collection of Evidence

By contrast, the corresponding treatment in the ISF SGP is defined in 22 pages and consists of 9 topics and a total of 74 subtopics, as shown in Table 1.7. For additional guidance, each topic in Table 1.6 is labeled as fundamental or specialized; links to documents at the ISF website provide related background and technical tutorial information. An organization that makes use of all this information can have significant confidence that it is effectively deploying the security controls needed to meet the requirement.

TABLE 1.7 The SGP Threat and Incident Management Category

Area	Topic	Number of Subtopics	Type
Cyber Security Resilience	Technical Vulnerability Management	10	Fundamental
	Security Event Logging	7	Fundamental
	Security Event Management	11	Specialized
	Threat Intelligence	10	Specialized
	Cyber Attack Protection	8	Specialized
Security Incident Management	Security Incident Management Framework	7	Fundamental
	Security Incident Management Process	5	Fundamental
	Emergency Fixes	7	Fundamental
	Forensic Investigations	9	Specialized

1.6 NIST Cybersecurity Framework and Security Documents

NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to the U.S. government and to the promotion of U.S. private sector innovation. Despite their national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact. In the area of information security, the NIST Computer Security Resource Center (CSRC) is the source of a vast collection of documents that are widely used in the industry.

NIST Computer Security Resource Center (CSRC) http://csrc.nist.gov

https://t.me/learningnets

NIST Cybersecurity Framework

NIST Cybersecurity
https://www.nist.gov/topics/cybersecurity

In response to the growing number of cyber intrusions at U.S. federal agencies, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* [EO13], directed the NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The resulting NIST Cybersecurity Framework [NIST18] includes leading practices that a variety of standards bodies have deemed successful. Thus, the framework is a collection of best practices—practices that improve efficiency and protect constituents. Although provided for federal agencies, the document is of use for nongovernment organizations.

The NIST Cybersecurity Framework consists of three components (see Figure 1.5):

- **Core:** Provides a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors
- **Implementation tiers:** Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk
- **Profiles:** Represents the outcomes based on business needs that an organization has selected from the Framework Core categories and subcategories

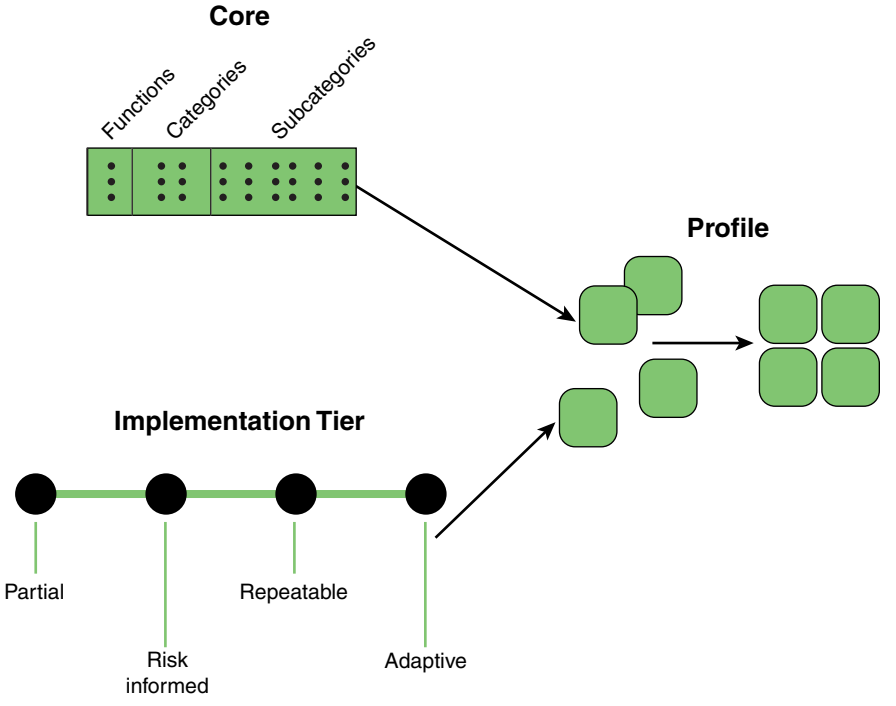


FIGURE 1.5 NIST Cybersecurity Framework Components

https://t.me/learningnets

The Framework Core identifies five key functions that comprise an organization's cybersecurity risk management approach. As shown in Table 1.8, each function is divided into a number of specific categories, each of which in turn is divided into a number of more detailed subcategories, for a total of 23 categories and 106 subcategories. The five functions provide a high-level view of the elements that comprise risk management for an organization. The categories are groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Each category is divided into subcategories of specific outcomes of technical and/or management activities that provide a set of results that, while not exhaustive, help support achievement of the outcomes in each category. For each subcategory the NIST Cybersecurity Framework provides a list of informative references, which are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate methods of achieving the outcomes associated with each subcategory.

TABLE 1.8 NIST Cybersecurity Framework Functions and Categories

Function	Description	Category
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services	Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	Response Planning Communications Analysis Mitigation Improvements
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event	Recovering Planning Improvements Communications

The Framework Core is intended not so much as a checklist of actions to be performed as a planning tool, enabling decision makers to more clearly appreciate what goes

https://t.me/learningnets

into effective risk management and to determine policies that emphasize the specific activities that are appropriate for the security goals of the organization.

The tiers defined in the Cybersecurity Framework help an organization define the priority that is to be given to cybersecurity and the level of commitment that the organization intends to make. The tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe increasing degrees of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and integrated into an organization's overall risk management practices (see Table 1.9).

TABLE 1.9 Cybersecurity Framework Implementation Tiers

Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1: Partial		
Risk management practices are not formalized but are, rather, ad hoc. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	Limited awareness of risk, no organizationwide approach to risk management or cybersecurity information to be shared within the organization.	Lack of coordination and collaboration with other entities.
Tier 2: Risk Informed		
Risk management practices are approved by management but not established as organizationwide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements	Processes and procedures are defined and implemented, and staff have adequate resources to perform their cybersecurity duties. No organizationwide approach to risk management.	No formal coordination and collaboration with other entities.
Tier 3: Repeatable		
Risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on changes in business/mission requirements and the threat and technology landscape.	Organizationwide approach to RM. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	Collaboration with partners enables risk management decisions in response to external events.

https://t.me/learningnets

Risk Management Process	Integrated Risk Management Program	External Participation
Tier 4: Adaptive		
Organization actively adapts to the changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.	Organizationwide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.	Organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

Once an organization has clarity on the degree of commitment to risk management (tiers) and an understanding of the actions that can be taken to match that commitment, security policies and plans can be put in place, as reflected in a Framework *profile*. In essence, a profile is a selection of categories and subcategories from the Framework Core. A current profile reflects the cybersecurity posture of the organization. Based on a risk assessment, an organization can define a target profile and then categories and subcategories from the Framework Core to reach the target. This definition of *current* and *target* profiles enables management to determine what has been done and needs to be maintained and what new cybersecurity measures need to be implemented to manage risk. The referenced guidelines, standards, and practices for each subcategory provide concrete descriptions of the work needed to meet the target profile.

The NIST Cybersecurity Framework is an important resource for those involved in the planning, implementation, and evaluation of an organization's cybersecurity capability. It is concise and uses clearly defined categories and subcategories. Approaching a document such as the ISF SGP or the ISO 27002 can be intimidating and even overwhelming because of the large body of knowledge they contain. The Cybersecurity Framework is an excellent resource to help an organization more effectively use these more detailed documents.

NIST Security Documents

NIST has produced a large number of FIPS publications and SPs that are enormously useful to security managers, designers, and implementers. Some of these documents are prescriptive standards, but many of them are tutorials or surveys and provide a continually updated source of educational material on a broad range of security topics. This section mentions some of the most important ones.

https://t.me/learningnets

countermeasure
An action, a device, a procedure, or a technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

By far the most significant of these documents is SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document lists management, operational, and technical safeguards or **countermeasures** prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Although intended for U.S. government systems, it is of equal applicability to IT systems in any organization. State-of-the-practice security controls and control enhancements have been integrated into the latest revision (2013) to address the evolving technology and threat space. Examples include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threats; and trustworthiness, assurance, and resilience of information systems. The revision also features eight new families of privacy controls that are based on the internationally accepted fair information practice principles.

Other documents of special interest include:

- **FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (2006):** Specifies minimum security requirements in 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.
- **SP 800-100, *Information Security Handbook: A Guide for Managers* (2006):** Provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Its topical coverage overlaps considerably with ISO 27002.
- **SP 800-55, *Performance Measurement Guide for Information Security* (2008):** Provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures.
- **SP 800-27, *Engineering Principles for Information Technology Security: A Baseline for Achieving Security* (2004):** Presents a list of system-level security principles to be considered in the design, development, and operation of an information system.
- **SP 800-12, *Introduction to Information Security*, (2017):** Provides an outstanding introduction to the topic of information security.
- **SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*:** Addresses the important security/privacy issues involved in moving data and applications to the cloud.

Recently, NIST introduced a new series of publications designated SP 1800. This new series, created to complement the SP 800 series, targets specific cybersecurity challenges in the public and private sectors and provides practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity.

https://t.me/learningnets

1.7 The CIS Critical Security Controls for Effective Cyber Defense

The Center for Internet Security (CIS) is a nonprofit community of organizations and individuals seeking actionable security resources. The CIS identifies specific security techniques and practices that the CIS group of experts agree are important.



Center for Internet Security https://www.cisecurity.org

A major contribution of CIS is The CIS Critical Security Controls for Effective Cyber Defense (CSC) [CIS18]. CSC focuses on the most fundamental and valuable actions that every enterprise should take. Value here is determined by knowledge and data—the ability to prevent, alert, and respond to the **attacks** plaguing enterprises today. CSC is significant for the real-world, practical nature of its information. It is not simply a list of controls that might be useful but a source that can be used to guide implementation of policy. The introduction to the CSC indicates that the controls have been matured by an international community of individuals and institutions that:

attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action.
- Document stories of adoption and share tools to solve problems.
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions/
- Map the CIS controls to regulatory and compliance frameworks and bring collective priority and focus to them.
- Share tools, working aids, and translations.
- Identify common problems (like initial assessment and implementation roadmaps) and solve them as a community.

The controls were developed as a result of members' experience with actual attacks and defenses that proved effective. The controls listed in the CSC are designed to be the most effective and specific technical measures available to detect, prevent, respond to, and mitigate damage from the most common to the most advanced attacks.

The bulk of the document is the presentation of 20 controls that encompass the broad range of known threats and the state of the art in countering those threats (see Table 1.10).

https://t.me/learningnets

TABLE 1.10 The CIS CSC List of Controls

Basic CIS Controls	Foundational CIS Controls	Organizational CIS Controls
CSC 1: Inventory and Control of Hardware Assets	CSC 7: Email and Web Browser Protections	CSC 17: Implement a Security Awareness and Training Program
CSC 2: Inventory and Control of Software Assets	CSC 8: Malware Defenses	CSC 18: Application Software Security
CSC 3: Continuous Vulnerability Management	CSC 9: Limitation and Control of Network Ports, Protocols, and Services	CSC 19: Incident Response and Management
CSC 4: Controlled Use of Administrative Privileges	CSC 10: Data Recovery Capability	CSC 20: Penetration Tests and Red Team Exercises
CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	CSC 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	
CSC 6: Maintenance, Monitoring and Analysis of Audit Logs	CSC 12: Boundary Defense	
	CSC 13: Data Protection	
	CSC 14: Controlled Access Based on the Need to Know	
	CSC 15: Wireless Access Control	
	CSC 16: Account Monitoring and Control	

Each control section includes the following:

- A description of the importance of the control in blocking or identifying the presence of attacks and an explanation of how attackers actively exploit the absence of this control
- A chart of the specific actions, called sub-controls, that organizations are taking to implement, automate, and measure the effectiveness of this control
- Procedures and tools that enable implementation and automation
- Sample entity relationship diagrams that show components of implementation

In addition, a companion document, *A Measurement Companion to the CIS Critical Security Controls*, describes techniques for measuring the performance of a given sub-control, plus a set of three risk threshold values (lower, moderate, and higher). The risk threshold values reflect the consensus of experienced practitioners.

https://t.me/learningnets

1.8 COBIT 5 for Information Security

Control Objectives for Business and Related Technology (COBIT) is a set of documents published by ISACA, which is an independent, nonprofit, global association engaged in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. COBIT 5, the fifth version of the set of documents to be released, is intended to be a comprehensive framework for the governance and management of enterprise IT. Of particular concern for this book is the section of COBIT 5 that deals with information security.



COBIT 5
http://www.isaca.org/cobit/pages/default.aspx

COBIT 5 for information security defines a number of policies that are used to develop a management and governance strategy. Table 1.11 lists the key functions associated with each policy.

TABLE 1.11 COBIT 5 for Information Security: Main Policies and Functions

Policy	Key Functions
Business continuity and disaster recovery	■ Business impact analysis (BIA) ■ Business contingency plans with trusted recovery ■ Recovery requirements for critical systems ■ Defined thresholds and triggers for contingencies, escalation of incidents ■ Disaster recovery plan (DRP) ■ Training and testing
Asset management	■ Data classification ■ Data ownership ■ System classification and ownership ■ Resource utilization and prioritization ■ Asset life cycle management ■ Asset protection measures
Rules of behavior (acceptable use)	■ At-work acceptable use and behavior ■ Off-site acceptable use and behavior
Information systems acquisition, software development, and maintenance	■ Information security in the life cycle process ■ Information security requirements definition process ■ Information security within the procurement/acquisition process ■ Secure coding practices ■ Integration of information security with change management and configuration management
Vendor management	■ Contract management ■ Information security terms and conditions ■ Information security evaluation ■ Monitoring of contracts for information security compliance
Communication and operation management	■ IT information security architecture and application design ■ SLA ■ IT information security operational procedures

https://t.me/learningnets

Policy	Key Functions
Compliance	■ IT information security compliance assessment process: ■ Development of metrics ■ Assessment repositories
Risk management	■ Organizational risk management plan ■ Information risk profile

COBIT 5 also provides a useful organization of the techniques used to achieve effective security into 5 domains and 37 processes, under two general categories, as follows:

- Governance of Enterprise IT
  - Evaluate, Direct and Monitor (EDM): 5 processes
- Management of Enterprise IT
  - Align, Plan and Organize (APO): 13 processes
  - Build, Acquire and Implement (BAI): 10 processes
  - Deliver, Service and Support (DSS): 6 processes
  - Monitor, Evaluate and Assess (MEA): 3 processes

Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options; setting direction through prioritization and decision making; and monitoring performance, compliance, and progress against agreed-on direction and objectives. Management plans, builds, runs, and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

1.9 Payment Card Industry Data Security Standard (PCI DSS)

The PCI-DSS, a standard of the PCI Security Standards Council, provides guidance for maintaining payment security. The standard sets the technical and operational requirements for organizations accepting or processing payment transactions and for software developers and manufacturers of applications and devices used in those transactions. In essence, PCI DSS compliance governs the way payment card data is processed, handled, and stored. It is required for merchants and all businesses that touch payment data in any way—and that's a lot of businesses.

https://t.me/learningnets

The PCI defines the scope of the PCI DSS as follows:

> The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.



PCI Security Standards Council https://www.pcisecuritystandards.org/pci_security/

The PCI DSS is structured around 6 goals and 12 requirements, as shown in Table 1.12. Each requirement is further broken up into one or two levels of subrequirements, for which testing procedures and guidance are provided.

TABLE 1.12 PCI DSS Goals and Requirements

Goal	Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

The following is an example of a PCI subrequirement:

- **Subrequirement 8.1.2:** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- **Testing procedures:** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.

https://t.me/learningnets

- **Guidance:** To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.

As you can see, the specification is clear and straightforward. Taken together, the many subrequirements with their testing procedures and guidance provide a powerful tool for managing a cybersecurity capability in the context of the use of payment cards.

1.10 ITU-T Security Documents



ITU-T
https://www.itu.int/en/Pages/default.aspx

The International Telecommunication Union (ITU) is a United Nations specialized agency—hence the members of ITU-T are governments. The U.S. representation is housed in the Department of State. The ITU's charter states that it is "responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis." Its primary objective is to standardize, to the extent necessary, techniques and operations in telecommunications to achieve end-to-end compatibility of international telecommunication connections, regardless of the countries of origin and destination. The ITU Telecommunication Standardization Sector (ITU-T) fulfills the purposes of the ITU relating to telecommunications standardization by studying technical, operating, and tariff questions and adopting recommendations on them with a view to standardizing telecommunications on a worldwide basis.

ITU-T has developed thousands of recommendations organized into 23 series. Security-related recommendations are scattered throughout a number of these series, making it difficult to gain a unified view of what the ITU-T has to offer in the way of guidance and explanation related to cybersecurity. Table 1.13 summarizes the key topics on cybersecurity, information security, and network security covered in numerous recommendations. Although the ITU-T focus has traditionally been telecommunications and Internet service providers (ISPs), many of the security documents have broader applicability.

TABLE 1.13 Key Topics Covered by ITU-T Security Recommendations

Topic	Subtopics
Security requirements	Threats, risks, and vulnerabilities Personnel and physical security requirements Next-generation networks Security requirements for IPCablecom IPTV

https://t.me/learningnets

Topic	Subtopics
Security architectures	Open systems security architecture Security services Security architecture for end-to-end communications Availability of the network and its components Application-specific architectures Peer-to-peer security architectures Message security Network management architecture IPCablecom architecture IPTV
Security management	Information security management Risk management Incident handling Asset management Governance of information security Telecommunications management
Role of the directory	Directory concepts Public-key security mechanisms Privilege management infrastructure Protection of Directory information Privacy protection
Identity management and telebiometrics	Identity management Overview of identity management Key ITU-T identity management standards Telebiometrics Telebiometric authentication Security and safety aspects of telebiometrics Telebiometrics related to human physiology Telebiometrics in e-health and telemedicine
Examples of approaches to authentication and non-repudiation	Secure password-based authentication protocol with key exchange One-time password authentication Non-repudiation framework based on one-time password Delegated non-repudiation
Securing the network infrastructure	The telecommunications management network Securing monitoring and control activities Securing network operation activities and management applications Protection against electromagnetic threats Common security management services CORBA (Common Object Request Broker Architecture)-based security services
Some specific approaches to network security	Next-generation network security Mobile communications security Security for home networks IPCablecom Ubiquitous sensor networks

https://t.me/learningnets



ITU-T Recommendations https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

Topic	Subtopics
Cybersecurity and incident response	Cybersecurity information exchange Exchange of vulnerability information Discovery of cybersecurity information Incident handling
Application security	Voice over IP (VoIP) and multimedia IPTV DRM for cable television multiscreen Secure fax Web services Tag-based services
Countering common network threats	Spam Malicious code, spyware, and deceptive software Notification and dissemination of software updates
Security aspects of cloud computing	Key characteristics of cloud computing Generic cloud computing capabilities and services Emerging cloud services Security threats and security challenges to cloud computing

As a guide to understanding and using these recommendations, ITU-T maintains a security manual, *Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of existing ITU-T Recommendations for Secure Telecommunications*, most recently updated in 2015 [ITUT15].

1.11 Effective Cybersecurity

This section introduces a useful way of view the cybersecurity management process and discusses the role of the best practices and standards documents discussed throughout this chapter.

The Cybersecurity Management Process

An essential characteristic of cybersecurity provision is that it is not a single end that is attained but an ongoing process. The goal of effective cybersecurity is constantly receding as management strives to keep up with changes in the cyberspace ecosystem, which comprises technology, threat capability, applications, IT resources, and personnel. Figure 1.6, which is similar in nature to figures found in SP 800-53, ISF SGP, and X.1055 (*Risk Management and Risk Profile Guidelines for Telecommunication Organizations*), suggests the nature of the cybersecurity management process.

https://t.me/learningnets

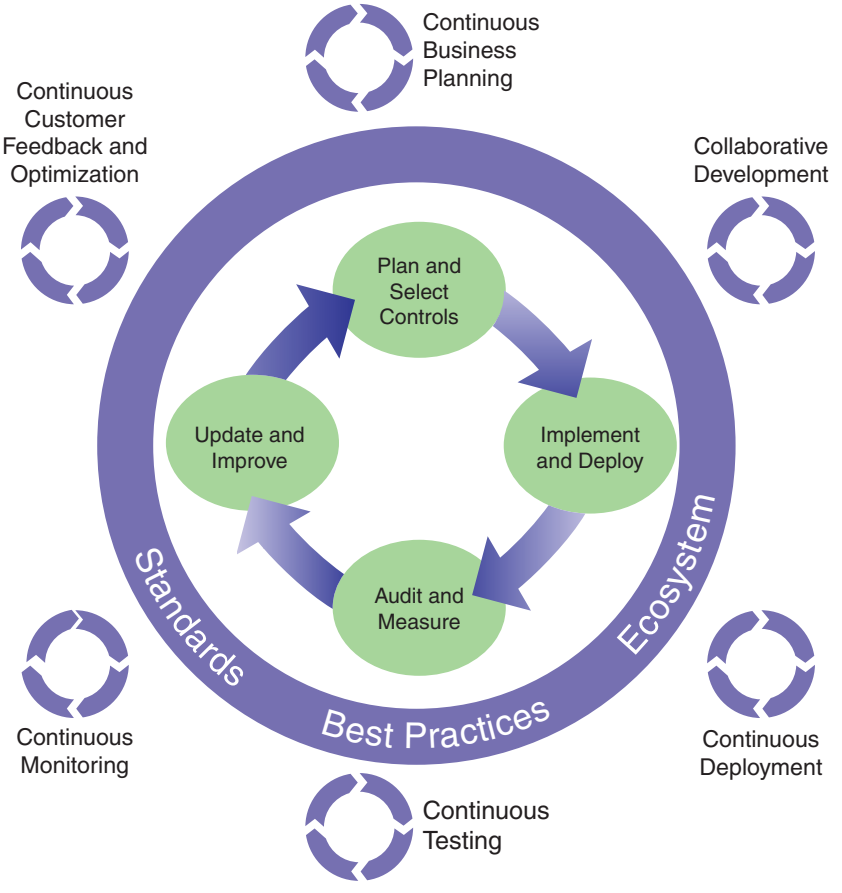


FIGURE 1.6 Cybersecurity Management Process

The process is a reiterative cycle with four major activities:

1. Assess the risk, considering the following:
    a. Assets and their value or utility
    b. Threats and vulnerabilities associated with these assets
    c. Risk of exposure of these assets to the threats and vulnerabilities
    d. Risk and impacts resulting from this risk of exposure

1b. Address the risk(s), considering the following:

a. Identification of available risk management options
b. Selection of preferred risk management option
c. Final risk management decision

https://t.me/learningnets

2. Implement the risk management decision, considering the following:
    a. Selection of controls
    b. Allocation of resources, roles, and responsibilities
    c. Implementation of controls
3. Monitor, review, and communicate the risks, considering the following:
    a. Monitoring of the risk situation
    b. Risk-related measurements
    c. Review and re-assessment of the risks
    d. Communication of the risks
4. Update and improve the controls:
    a. Updating controls
    b. Improving controls

This repeating cycle is governed not only by the evolving ecosystem of cyberspace but also by evolving standards and best practices.

At a broader perspective, there are in fact two cyclic processes at work: one at the executive level, which focuses on organizational risk, and one at the business level, which focuses on critical infrastructure risk management. Figure 1.7, similar to one in the NIST Cybersecurity Framework, illustrates this relationship. At the executive level, upper management defines mission priorities, establishes acceptable risk tolerance, and determines available resources. At the business level, IT management translates these guidelines into controls for risk management.

Using Best Practices and Standards Documents

This chapter reviews a broad range of documents available to cybersecurity planners and implementers. Although there is considerable overlap in these documents, recognizing the differences can make the use of these documents more effective. In terms of overall planning, perhaps the key resource is the NIST Cybersecurity Framework. It provides management with a clear methodology for developing a framework profile. This profile can then be used as a guide in assembling a suite of controls for risk management.

For purposes of putting together a set of cybersecurity controls, ISF SGP and ISO 27002 provide the most thorough guidance. In particular, the ISF SGP is a comprehensive survey of what is available to cybersecurity managers, implementers, and evaluators, taken to a thorough level of detail.

https://t.me/learningnets



FIGURE 1.7 Cybersecurity Information and Decision Flows Within an Organization

For choosing specific controls, the CIS Critical Security Controls document is invaluable as its details are based on broad real-world experience.

In addition, other documents, especially from NIST and ITU-T, provide broad coverage of cybersecurity topics, including tutorial-style presentations, recommendations in specific areas, and supporting material.

https://t.me/learningnets

1.12 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

accountability
asset
attack
authenticity
availability
certification
confidentiality
countermeasure
cyberspace
cybersecurity
cybersecurity framework
information security management system (ISMS)
integrity
non-repudiation
risk
security controls
security policy
security threat
threat
vulnerability

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Explain briefly each of the following terms from the perspective of cybersecurity: availability, integrity, authenticity, non-repudiation, confidentiality.
2. Enumerate three key challenges in developing an effective cybersecurity system and provide examples of each one.
3. Name a few technologies commonly implemented for cybersecurity in large organizations.
4. What is the most significant activity of the Information Security Forum (ISF)?
5. What are the three key activities for information security as per the Standard of Good Practice for Information Security?
6. Explain what the term ISMS stands for and what it means.
7. Explain briefly the five core functions in the NIST Cybersecurity Framework.
8. Which is the weakest area of information security in any organization?

https://t.me/learningnets

1.13 References

CICE14: Cicerone, R., & Nurse, P. (Eds.), *Cybersecurity Dilemmas: Technology, Policy, and Incentives.* National Academy of Sciences, 2014.

CIS18: Center for Internet Security, *The CIS Critical Security Controls for Effective Cyber Defense version 7.* 2018. https://www.cisecurity.org

CLAR14: Clark, D., Berson, T., & Lin, H. (Eds.), *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* National Research Council, National Academy of Sciences, 2014.

EO13: Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." *Federal Register*, February 19, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

ITUT15: ITU-T, *Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications*. September 2015.

LAMB06: Lambo, T., "ISO/IEC 27001: The Future of Infosec Certification." *ISSA Journal*, November 2006.

NIST18: NIST. *Framework for Improving Critical Infrastructure Cybersecurity.* April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

https://t.me/learningnets

https://t.me/learningnets

PART I

Planning for Cybersecurity

Ah, miss, it is a pity you didn't let me know what you were planning, for I would have told you that your pains were wasted.

— *The Adventure of the Copper Beaches,* Sir Arthur Conan Doyle

Everyone has a plan 'till they get punched in the face.

— Mike Tyson

CHAPTER 2: Security Governance
CHAPTER 3: Information Risk Assessment
CHAPTER 4: Security Management

Part I provides an overview of approaches for managing and controlling the cybersecurity function; defining the requirements specific to a given IT environment; and developing policies and procedures for managing the security function. **Chapter 2** introduces the concept of information security governance. The chapter discusses how security governance enables the direction and oversight of information security-related activities across an enterprise, as an integrated part of corporate governance. **Chapter 3** discusses the range of issues dealing with defining security requirements for an organization and developing procedures to ensure compliance. **Chapter 4** focuses on security issues that are primarily related to the internal policies and operation of an organization. This includes: (a) security policy and organization: issues related to defining a comprehensive security policy, keeping it up to date, and effectively communicating it; and (b) information security management: issues relating to the management of the information security function, to ensure good practice in information security is applied effectively and consistently throughout the organization.

https://t.me/learningnets

Chapter 2

Security Governance

A prince or general can best demonstrate his genius by managing a campaign exactly to suit his objectives and his resources, doing neither too much nor too little. But the effects of genius show not so much in novel forms of action as in the ultimate success of the whole.

—*On War*, Carl Von Clausewitz

Learning Objectives

After studying this chapter, you should be able to:

- Explain the concept of security governance and how it differs from security management.
- Provide an overview of the key components of security governance.
- Discuss the topics that should be covered in a strategic security plan.
- Discuss the topics that should be covered in an information security report.
- Explain the roles and responsibilities that are part of security governance.
- Present an overview of the concepts of information security architecture.
- Present an overview of security governance best practices.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, defines information security governance as follows:

Information security governance

The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

https://t.me/learningnets

ITU-T X.1054, *Governance of Information Security*, defines information security governance as "the system by which an organization's information security-related activities are directed and controlled."

More generally, the term *security governance* encompasses **governance** concerns for cybersecurity, information security, and network security.

governance
Establishment of policies and continuous monitoring of their proper implementation by the members of the governing body of an organization. Governance includes the mechanisms required to balance the powers of the members (with the associated accountability) and their primary duty of enhancing the prosperity and viability of the organization.

2.1 Security Governance and Security Management

To better understand the role of security governance, it is useful to distinguish between information security governance (previously defined), information security management, and information security implementation/operations. ISO 27000 defines **information security management** as follows:

> The supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

And **information security implementation/operations** can be defined in this fashion:

> The implementation, deployment and ongoing operation of security controls defined within a cybersecurity framework.

Figure 2.1 suggests the hierarchical relationship between these three concepts. The security governance level communicates the mission priorities, available resources, and overall risk tolerance to the security management level. In essence, security governance is the process of developing a **security program** that adequately meets the strategic needs of the business. The security management level uses the information as inputs into the risk management process that realizes the security program. It then collaborates with the implementation/operations level to communicate security requirements and create a cybersecurity profile. The implementation/operations level integrates this profile into the system development life cycle and continuously monitors security performance. It executes or manages security-related processes related to current infrastructure on a day-to-day basis. The security management level uses monitoring information to assess the current profile and reports the outcomes of that assessment to the governance level to inform the organization's overall risk management process.

security program
The management, operational, and technical aspects of protecting information and information systems. A security program encompasses policies, procedures, and management structure and mechanism for coordinating security activity.

https://t.me/learningnets

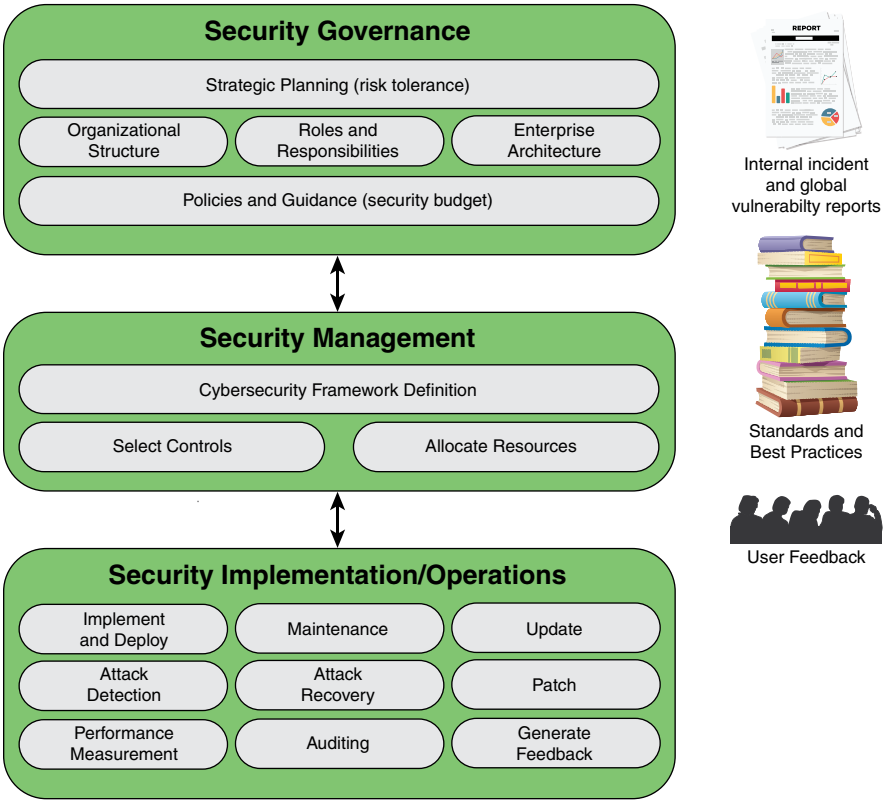


FIGURE 2.1 Information Security Management System Element

Figure 2.1 illustrates the key responsibilities at each level. As indicated, there is interaction among the three layers in the ongoing evolution of the information security management system (ISMS). In addition, three supplemental factors play roles. Internal security incident reports and global vulnerability reports from various sources help define the threat and level of risk that the organization faces in protecting its information assets. The numerous standards and best practices documents provide guidance on managing risk. User feedback comes from both internal users and external users who have access to the organization's information assets. This feedback helps improve the effectiveness of policies, procedures, and technical mechanisms. Depending on the organization and its cybersecurity approach, each of the three factors plays a role to a greater or lesser extent at each level.

This chapter is devoted to security governance. Chapter 3, "Information Risk Assessment," covers security management, and the succeeding chapters cover security implementation/operations.

https://t.me/learningnets

2.2 Security Governance Principles and Desired Outcomes

Before getting into the details of security governance, an overview of principles and desired outcomes provides useful context.

Principles

X.1054 provides concepts and guidance on principles and processes for information security governance, by which organizations evaluate, direct, and monitor the management of information security. X.1054 lays out as a key objective of information security governance the alignment of information security objectives and strategy with overall business objectives and strategy. X.1054 lists six principles for achieving this objective:

- **Establish organizationwide information security.** Information security, or cybersecurity, concerns should permeate the organization's structure and functions. Management at all levels should ensure that information security is integrated with **information technology (IT)** and other activities. Top-level management should ensure that information security serves overall business objectives and should establish responsibility and accountability throughout the organization.
- **Adopt a risk-based approach.** Security governance, including allocation of resources and budgets, should be based on the risk appetite of an organization, considering loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss.
- **Set the direction of investment decisions.** Information security investments are intended to support organizational objectives. Security governance entails ensuring that information security is integrated with existing organization processes for capital and operational expenditure, for legal and regulatory compliance, and for risk reporting.
- **Ensure conformance with internal and external requirements.** External requirements include mandatory legislation and regulations, standards leading to certification, and contractual requirements. Internal requirements comprise broader organizational goals and objectives. Independent security audits are the accepted means of determining and monitoring conformance.
- **Foster a security-positive environment for all stakeholders.** Security governance should be responsive to **stakeholder** expectations, keeping in mind that various stakeholders can have different values and needs. The governing body

information technology (IT)
Applied computer systems, both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. IT is often the name of the part of an enterprise that deals with all things electronic.

stakeholder
A person, a group, or an organization that has interest or concern in an organization. Stakeholders can affect or can be affected by the organization's actions, objectives, and policies. Some examples of stakeholders are creditors, directors, employees, government (and its agencies), owners (shareholders), suppliers, unions, and the community from which the business draws its resources.

https://t.me/learningnets

should take the lead in promoting a positive information security culture, which includes requiring and supporting security education, training, and awareness programs.

- **Review performance in relation to business outcomes.** From a governance perspective, security performance encompasses not just effectiveness and efficiency but also impact on overall business goals and objectives. Governance executives should mandate reviews of a performance measurement program for monitoring, audit, and improvement that links information security performance to business performance.

Adherence to these principles is essential to the success of information security in the long term. How these principles are to be satisfied and who is responsible and accountable depend on the nature of the organization.

Desired Outcomes

The IT Governance Institute defines five basic outcomes of information security governance that lead to successful integration of information security with the organization's mission [ITGI06]:

- **Strategic alignment**: The support of strategic organizational objectives requires that information security strategy and policy be aligned with business strategy.
- **Risk management**: The principal driving force for information security governance is risk management, which involves mitigating risks and reducing or preventing potential impact on information resources.
- **Resource management**: The resources expended on information security (e.g., personnel time and money) are somewhat open ended and a key goal of information security governance is to align information security budgets with overall enterprise requirements.
- **Value delivery**: Not only should resources expended on information security be constrained within overall enterprise resource objectives, but also information security investments need to be managed to achieve optimum value.
- **Performance measurement**: The enterprise needs metric against which to judge information security policy to ensure that organizational objectives are achieved.

It is worthwhile to keep these outcomes in mind throughout the discussion in the remainder of the chapter.

https://t.me/learningnets

2.3 Security Governance Components

SP 800-100 lists the following key activities, or components that constitute effective security governances (refer to Figure 2.1):

- Strategic planning
- Organizational structure
- Establishment of roles and responsibilities
- Integration with the enterprise architecture
- Documentation of security objectives in policies and guidance

The following sections examine each of these components in turn.

Strategic Planning

It is useful for this discussion to define three hierarchically related aspects of strategic planning (see Figure 2.2):

- Enterprise strategic planning
- Information technology (IT) strategic planning
- Cybersecurity or information security strategic planning

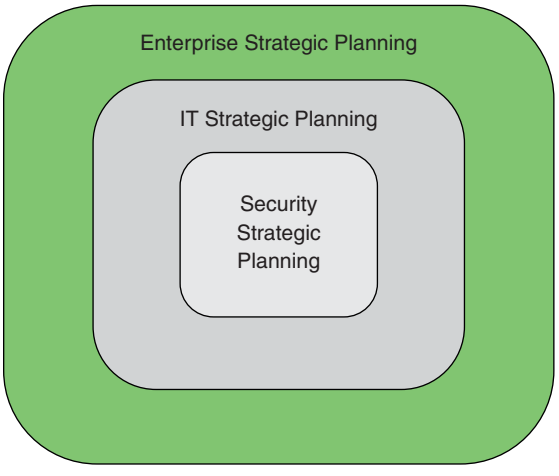


FIGURE 2.2 Strategic Planning

Enterprise strategic planning involves defining long-term goals and objectives for an organization (for example, business enterprise, government agency, or nonprofit

https://t.me/learningnets

strategic plan
A document used to communicate, within the organization, the organization's goals, the actions needed to achieve those goals, and all the other critical elements developed during planning exercises.

organization) and the development of plans to achieve these goals and objectives. The management activity involved in enterprise strategic planning is described in the Strategic Management Group's *Strategic Planning Basics* [SMG17] as an activity used to set priorities, focus energy and resources, strengthen operations, ensure that employees and other stakeholders are working toward common goals, establish agreement around intended outcomes/results, and assess and adjust the organization's direction in response to a changing environment. It involves the development of a **strategic plan** and the ongoing oversight of the implementation of that plan.

IT strategic planning is the alignment of IT management and operation with enterprise strategic planning. The need to move beyond IT management and to ensure that the IT planning process is integrated with enterprise strategic planning follows from two strategic factors: mission necessity and enterprise maturity [JUIZ15]. With many actors exploiting IT to maximize effectiveness, an organization must engage in strategic planning to ensure that investments in IT produce business value and that the assessment of risks is aligned with enterprise goals and objectives. This is a necessity to support the overall enterprise mission. Further, as the IT infrastructure develops and matures, meeting enterprise strategic goals is likely to involve new arrangements with outside providers, such as cloud service providers, more use of mobile devices by employees and outside actors, and perhaps reliance on a variety of new hardware and software to develop Internet of Things (IoT) capability. These activities may create unintended barriers to flexibility and introduce new areas of risk. IT management must be guided by strategic planning to meet these challenges.

One of the best-documented examples of IT strategic planning is the process used at Intel [HAYD08a, HAYD08b, PETE12]. It is worth examining this model because it also serves as a model for security strategic planning. Intel's IT strategic planning process comprises six phases, as shown in Figure 2.3.

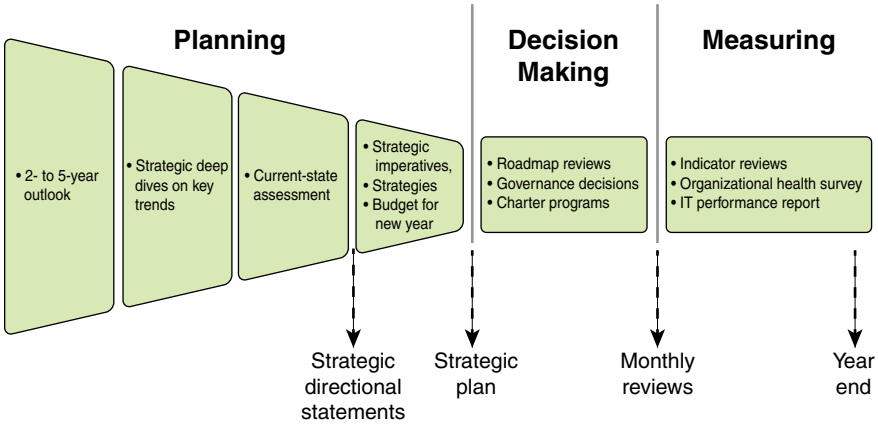


FIGURE 2.3 Intel's IT Strategic Planning Process

https://t.me/learningnets

The six phases are as follows:

1. **Two- to five-year business and technology outlook:** At the beginning of the year, the planning team takes as input an overall vision and mission statement developed at the enterprise level. During this phase, the team reviews the enterprise strategies, technology trends, employee trends, and so on to better understand the future environment that will shape the IT organization and its deliverables. IT subject matter experts from throughout the organization are recruited to help define the major trends that may be critical in shaping the organization and its decision making in the next few years.
2. **Strategic deep dive:** The team identifies a small number of high-impact areas that require more in-depth analysis to inform the overall strategic planning process. Depending on circumstances at a given point in time, these may include IoT, social media trends, and changing regulatory compliance rules.
3. **Current-state assessment:** The planning team analyzes the current state of all the IT-related systems and policies and compares these with the long-range outlook, paying special attention to the key drivers developed in the preceding phase. The result is a set of recommendations for adjustments to IT's focus areas and spending plans.
4. **Imperatives, roadmaps, and finances:** The next phase is the development of a strategic plan for IT. The plan includes a discussion of strategic objectives and a budget and investment plan. The plan reflects IT's highest-priority items and provides an outcome framework for defining success. Each item includes a roadmap that can influence budget and organization decisions in the upcoming year.
5. **Governance process and decision making:** Once the annual budget is approved, the information from the preceding phases is used to guide the governance process and the many decisions made across the organization to implement the strategic plan and one-year strategic objectives. These decisions include project chartering, supplier selection, sourcing, investment trade-off decisions, and so on.
6. **Regular reviews:** Monthly reviews based on a wide variety of input help ensure that the strategic plan and governance decisions are followed. This culminates in a year-end assessment. Reviews continue into the following year until a new strategic plan and new governance decisions provide input for modifying the review process.

This process can include a security strategic planning component, or planning can occur in a coordinated and parallel fashion in another team.

https://t.me/learningnets

Information security strategic planning is alignment of information security management and operation with enterprise and IT strategic planning. The pervasive use and value of IT within organizations has resulted in an expanded notion of IT's delivery of value to the organization to include mitigation of the organization's risk [ZIA15]. Accordingly, IT security is a concern at all levels of an organization's governance and decision-making processes, and information security strategic planning is an essential component of strategic planning.

An information security strategic plan should be embodied in a document that is approved by the appropriate executives and committees and is regularly reviewed. Table 2.1 suggests an outline for such a document.

TABLE 2.1 Elements of a Strategic Plan Document

Section	Description
Definition	
Mission, vision, and objectives	Defines the strategy for aligning the information security program with organizational goals and objectives, including the role of individual security projects in enabling specific strategic initiatives.
Priorities	Describes factors that determine strategy and the priorities of objectives.
Success criteria	Defines success criteria for the information security program. Includes risk management, resilience, and protection against adverse business impacts.
Integration	Strategy for integrating the security program with the organization's business and IT strategy.
Threat defense	Describes how the security program will help the organization defend against security threats.
Execution	
Operations plan	An annual plan to achieve agreed objectives that involves agreeing on budgets, resources, tools, policies, and initiatives. This plan (a) can be used for monitoring progress and communicating with stakeholders and (b) ensures that information security is included from the outset in each relevant project.
Monitoring plan	This plan involves planning and maintaining a stakeholder feedback loop, measuring progress against objectives, and ensuring that strategic objectives remain valid and in line with business needs.
Adjustment plan	This plan involves ensuring that strategic objectives remain valid and in line with business needs as well as procedures to communicate the value.
Review	
Review plan	This plan describes procedures and individuals/committees involved in regular review of the information security strategy.

https://t.me/learningnets

Organizational Structure

The organizational structure to deal with cybersecurity depends, in large part, on the size of the organization, its type (for example, government agency, business, nonprofit), and the organization's degree of dependence on IT. But the essential security governance functions to be performed are in essence the same across organizations. Figure 2.4, which is based on a figure in X.1054, illustrates these basic functions within a broader context.

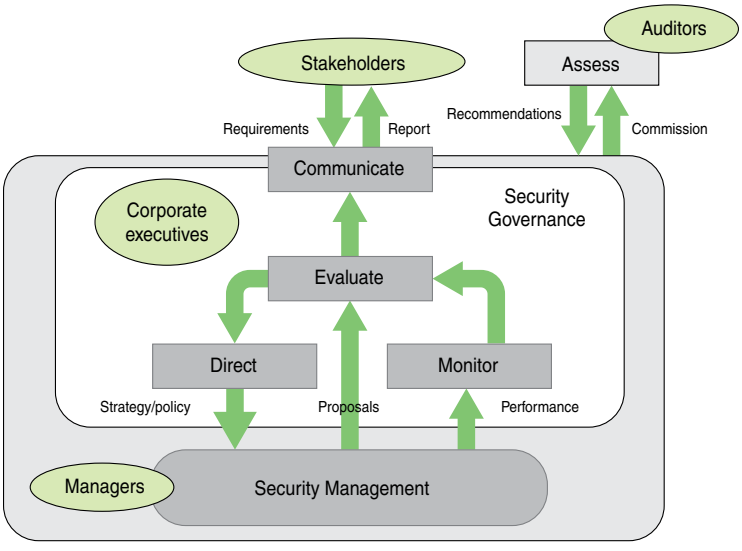


FIGURE 2.4 Framework for Security Governance

The basic security governance functions are as follows:

- **Direct:** Guiding security management from the point of view of enterprise strategies and risk management. This function involves developing an information security policy.
- **Monitor:** Monitoring the performance of security management with measurable indicators.
- **Evaluate:** Assessing and verifying the results of security performance monitoring in order to ensure that objectives are met and to determine future changes to the ISMS and its management.
- **Communicate:** Reporting enterprise security status to stakeholders and evaluating stakeholder requirements.

https://t.me/learningnets

This framework includes the governing cycle to direct, monitor, and evaluate the ISMS. The evaluation incorporates both the results of the monitoring and proposals from security management to dictate changes and improvements. This cycle is in accordance with Requirement 4.4 in ISO 27001 that the organization shall establish, implement, maintain, and continually improve an ISMS.

The evaluate function triggers communication with stakeholders in the form of a report, which can be issued annually, more frequently, or based on a security incident. As indicated in the Information Security Governance Framework [OHKI09], reporting to stakeholders serves two purposes:

- **Accountability:** Reporting enables stakeholders to ensure that information security is being managed effectively, and it should include the following:
  - Information security policy
  - Risk evaluation
  - Risk measures and response
  - Management systems
- **Effect on corporate value:** Reporting should disclose the following:
  - Estimates of the costs and benefits of making an inventory of information assets. The information security risk assessment process includes making a complete inventory of information assets. This inventory may support improved strategic management of the information assets, apart from security concerns, which may enhance corporate value.
  - Estimates of the value of an inventory of information assets that is developed as a result of information security activities.
  - The extent to which information security activities increase the brand value as well as the trust of the customers and partners.
  - The economic value of protected information assets.
  - The amount by which the security implementation reduces the risk of damaging the information assets.

The following sidebar provides an example of an information security report outline, from the Information Security Governance Framework [OHKI09]. This report structure is based on a study of private companies by the Japanese Ministry of Economics, Trade and Industry. It gives an overall picture of the enterprise's information security governance. Section 5, in particular, involves providing a status update, which should be in sufficient detail for stakeholders to determine whether information security activities are being carried out as planned.

https://t.me/learningnets

Information Security Report

(1) **Basic Information**
Includes the purpose of issue of the report, cautions relating to usage, target periods and responsible departments.

(2) **Concept of Management Regarding Information Security**
Includes policy regarding information-security undertakings, target scope, ranking of stakeholders in the report and messages to stakeholders.

(3) **Information Security Governance**
Information security management system (e.g., placement of responsibility, organizational structure and compliance), risks relating to information security and information security strategy.

(4) **Information Security Measures Planning and Goals**
Includes action plan and target values.

(5) **Results and Evaluation of Information Security Measures**
Includes results, evaluation, information security quality improvement activities, management of overseas bases, outsourcing, social contribution activities relating to information security and accident reports.

(6) **Principle Focal Themes Relating to Information Security**
Includes internal controls and protection of personal information, undertakings to be particularly emphasized such as Business Continuity Plans, introduction to themes and newly devised points.

(7) **Third-Party Approval, Accreditation, etc. (if Required)**
Includes ISMS compliance evaluation system, information security audits, privacy mark systems, number of persons with information security qualifications, classification, and ranking.

X.1054 provides an example of information security status report structure that includes the following detailed contents:

- Introduction
  - Scope (strategy, policies, standards), perimeter (geographic/organizational units), period covered (month/quarter/six months/year)
- Overall status
  - Satisfactory/not yet satisfactory/unsatisfactory

https://t.me/learningnets

- Updates (as appropriate and relevant)
  - Progress toward achieving the information security strategy
  - Elements completed/in-hand/planned
  - Changes in information security management system
  - ISMS policy revision, organizational structure to implement ISMS (including assignment of responsibilities)
  - Progress toward certification
  - ISMS (re)certification, certified information security audits
  - Budgeting/staffing/training
  - Financial situation, headcount adequacy, information security qualifications
  - Other information security activities
  - Business continuity management involvement, awareness campaigns, internal/external audit assistance
- Significant issues (if any)
  - Results of information security reviews
  - Recommendations, management responses, action plans, target dates
  - Progress in respect of major internal/external audit reports
  - Recommendations, management responses, action plans, target dates
  - Information security incidents
  - Estimated impact, action plans, target dates
  - Compliance (or noncompliance) with related legislation and regulations
  - Estimated impact, action plans, target dates
- Decision(s) required (if any)
  - Additional resources
  - To enable information security to support business initiative(s)

Such an outline is particularly useful for organizations that expect to enhance their reputation by emphasizing their security (for example, information and communications technology businesses). Transparency of the organization's approach to its security risk and appropriate disclosure is also effective at increasing trust. Common awareness can be shared among stakeholders through such activities. For example,

https://t.me/learningnets

public cloud service providers share considerable detail about the information security program and even go the extent of allowing customers to conduct audits and vulnerability testing with prior arrangement. Other service providers and organizations with business customers traditionally did not provided this level of transparency.

Finally, the assess function depicted in Figure 2.4 is performed by independent third-party auditors, commissioned by enterprise top management.

Roles and Responsibilities

A key aspect of security governance is defining the roles and responsibilities of executives related to information security. Typically, these are **C-level** executives. Executive positions that play a role in security governance include the following:

C-level

Chief level. Refers to high-ranking executives in an organization. Officers who hold C-level positions set the company's strategy, make high-stakes decisions, and ensure that the day-to-day operations align with fulfilling the company's strategic goals.

- **Chief executive officer (CEO):** Responsible for the success or failure of the organization, overseeing the entire operation at a high level.
- **Chief operating officer (COO):** Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations.
- **Chief information officer (CIO):** In charge of IT strategy and the computer, network, and third-party (for example, cloud) systems required to support the enterprise's objectives and goals.
- **Chief security officer (CSO)** or **chief information security officer (CISO):** Tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security and a CISO in charge of digital security.
- **Chief risk officer (CRO):** Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings. This role does not exist in most enterprises. It is most often found in financial service organizations. In enterprises in which a CRO is not present, organizational risk decisions may be the responsibility of the CEO or board of directors.
- **Chief privacy officer (CPO):** Charged with developing and implementing policies designed to protect employee and customer data from unauthorized access.

Figure 2.5 shows an example of reporting relationships among these roles for a large enterprise. In smaller organizations, a number of these roles may be assumed by a single individual.

https://t.me/learningnets

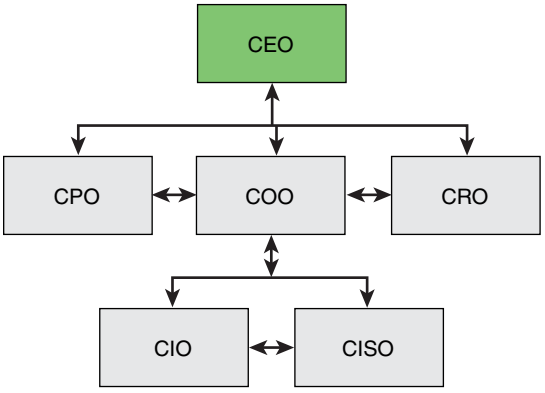


FIGURE 2.5 Possible Reporting Relationships for Security Governance

Two breakdowns of responsibility are useful in showing how to structure security-related roles in an organization. Figure 2.6, based on one in the Corporate Governance Task Force's *Information Security Governance: A Call to Action* [CGTF04], shows a recommended assignment of roles and responsibilities. This useful report also provides a more detailed discussion of these roles as well as a list of recommendations for implementing effective security governance.

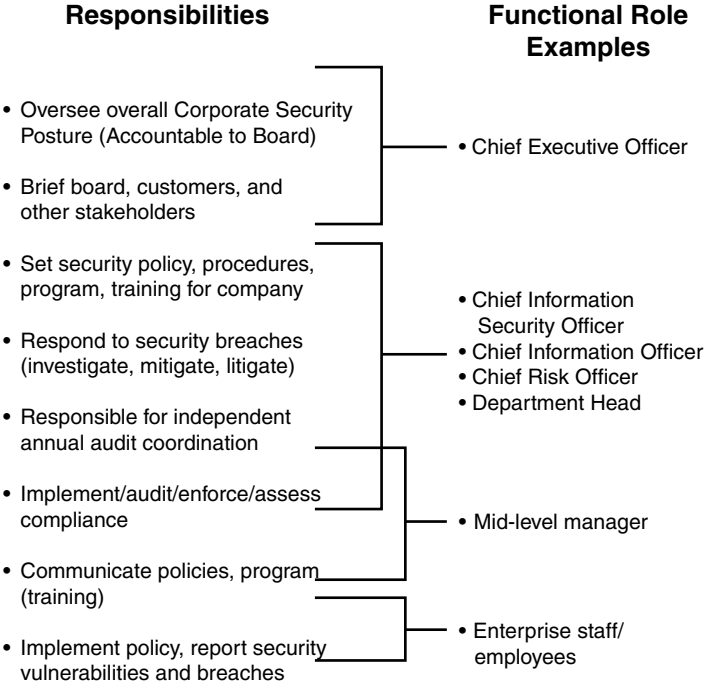


FIGURE 2.6 Security Governance Roles and Responsibilities Example

https://t.me/learningnets

The Business Software Alliance's *Information Security Governance: Toward a Framework for Action* [BSA03] proposes a governance framework based on three categories (see Table 2.2):

- **Governance/business drivers:** What am I required to do? What should I do?
- **Roles and responsibilities:** How do I accomplish my objectives?
- **Metrics/audit:** How effectively do I achieve my objectives? What adjustments do I need to make?

TABLE 2.2 Information Security Governance Responsibilities

Governance/ Business Drivers	Roles and Responsibilities	Metrics/Audit
Corporate Executive		
Legislation, ROI	■ Provide oversight and coordination of policies ■ Provide oversight of business unit compliance ■ Ensure compliance reporting ■ Monitor actions to enforce accountability	Financial reporting, monetizing losses, conforming to policies
Business Unit Head		
Standards, policies, budgets	■ Provide information security protection commensurate with the risk and business impact ■ Provide security training ■ Develop the controls environment and activities ■ Report on effectiveness of policies, procedures, and practices	Policy violations, misuse of assets, internal control violations
Senior Manager		
Standards, audit results	■ Provide security for information and systems ■ Periodic assessments of assets and their associated risks ■ Determine level of security appropriate ■ Implement policies and procedures to cost-effectively reduce risk to acceptable levels ■ Perform periodic testing of security and controls	Risk assessment and impact analysis, control environment activities, remedial actions, policy and procedure compliance, security and control test results

https://t.me/learningnets

Governance/ Business Drivers	Roles and Responsibilities	Metrics/Audit
CIO/CISO		
Security policies, security operations, and resources	■ Develop, maintain, and ensure compliance with the program ■ Designate a security officer with primary duties and training ■ Develop required policies to support the security program and business-unit-specific needs ■ Assist senior managers with their security responsibilities ■ Conduct security awareness training	Security awareness effectiveness, incident response and impact analysis, security program effectiveness, information integrity, effects on information processing

Integration with Enterprise Architecture

information security architecture
An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

A key element of security governance is the development of an **information security architecture**. This **architecture** provides information on how security capabilities (for example, identity and access management) are placed and used in the **enterprise architecture**. It allocates security requirements and controls to common services or infrastructures. It also provides a foundation for achieving risk-appropriate information system security, determining what circumstances and which security controls apply to information systems.

Over the past 20 years, a number of enterprise architecture models have been developed and adopted by various organizations. Two widely used governance resources for developing an information security architecture as part of an enterprise architecture are The Open Group Architecture Framework (TOGAF) [TOG11] and the Federal Enterprise Architecture Framework (FEAF) [OMB13]. The FEAF is the most comprehensive of all the enterprise architectures in use [SESS07], and this section provides an overview of it. Although developed for use by U.S. federal agencies, the FEAF is used effectively as a governance tool by other government organizations, private enterprises, nonprofit groups, and other organizations.

architecture
The way in which the component parts of an entity are arranged, organized, and managed.

The FEAF provides the following:

- A perspective on how enterprise architectures are viewed in terms of sub-architecture domains
- Six reference models for describing different perspectives of the enterprise architecture
- A process for creating an enterprise architecture

https://t.me/learningnets

- A transitional process for migrating from a pre-enterprise architecture to a post-enterprise architecture paradigm
- A taxonomy for cataloging assets that fall within the purview of the enterprise architecture
- An approach to measuring the success of using the enterprise architecture to drive business value

enterprise architecture
The systems, infrastructure, operations, and management of all information technology throughout an enterprise. The architecture is typically organized as high-level internally compatible representations of organizational business models, data, applications, and information technology infrastructure.

The sub-architecture domains represent specific areas of the overall framework. The domains provided a standardized language and framework for describing and analyzing investments and operations.

Each domain is defined in terms of a set of artifacts, which are essentially items of documentation that describe part or all of an architecture. [EAPA17] describes three levels of artifacts:

- **High-level artifacts**: These document strategic plans and objectives, typically in the form of policy statements and diagrams.
- **Mid-level artifacts**: These document organizational procedures and operations, such as services, supply chain elements, information flows, and IT and network architecture. Typical artifacts at this level are narrative description, flowcharts, spreadsheets, and diagrams.
- **Low-level EA artifacts**: These document the specific resources, such as applications, interfaces, data dictionaries, hardware, and security controls. Typical artifacts at this level are detailed technical specifications and diagrams.

The FEAF describes six domains:

- Strategy
- Business
- Data and information
- Enabling applications
- Host and infrastructure
- Security

Corresponding to the six domains are six reference models that describe the artifacts in the corresponding domains (see Table 2.3).

https://t.me/learningnets

TABLE 2.3 Enterprise Architecture Reference Models

Reference Model	Elements	Goals/Benefits
Performance reference model	Goals, measurement areas, measurement categories	Improved organizational performance and governance, cost benefits
Business reference model	Mission sectors, functions, services	Organization transformation, analysis, design, and reengineering
Data reference model	Domain, subject, topic	Data quality/reuse, information sharing, Agile development
Application reference model	System, component, interface	Application portfolio management, cost benefits
Infrastructure reference model	Platform, facility, network	Asset management standardization, cost benefits
Security reference model	Purpose, risk, control	Secure business/IT environment

The following description provides further detail of the reference models (RMs):

- **Performance reference model (PRM):** Defines standard ways of describing the value delivered by enterprise architectures, linked to the strategy domain. An example of a PRM artifact for this domain is a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis report that presents the strengths, weaknesses/limitations, opportunities, and threats involved in a project or in a business venture, including risks and impacts.
- **Business reference model (BRM):** Describes an organization through a taxonomy of common mission and support service areas. The BRM provides guidance in defining functions and services in various mission sectors of the enterprise and is linked to the business services domain. An example of a BRM artifact for this domain is a use-case narrative and diagram that describes a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal.
- **Data reference model (DRM):** Facilitates discovery of existing data holdings residing in silos and enables understanding the meaning of the data, how to access it, and how to leverage it to support performance results. The DRM is linked to the data and information domain. An example of a DRM artifact for this domain is a data dictionary, which is a centralized repository of information about data such as name, type, range of values, source, and authorization for access for each data element in the organization's files and databases.
- **Application reference model (ARM):** Categorizes the system- and application-related standards and technologies that support the delivery of service capabilities. The ARM provides guidance in developing a uniform scheme for documenting system, components, and interfaces and for managing

https://t.me/learningnets

application portfolios. It is linked to the enabling applications domain. An example of an ARM artifact for this domain is a system/application evolution diagram. This artifact documents the planned incremental steps toward migrating a suite of systems and/or applications to a more efficient suite, or toward evolving a current system or application to a future implementation.

- **Infrastructure reference model (IRM):** Categorizes the network- or cloud-related standards and technologies to support and enable the delivery of voice, data, video, and mobile service components and capabilities. The ARM provides guidance in developing a uniform scheme for documenting platform, facility, and network elements and managing assets. It is linked to the host infrastructure domain. An example of an IRM artifact for this domain is a hosting concept of operations, which presents the high-level functional architecture, organization, roles, responsibilities, processes, metrics, and strategic plan for hosting and use of hosting services. Other artifacts provide detailed documentation of infrastructure elements.
- **Security reference model (SRM):** Provides a common language and methodology for discussing security and privacy in the context of the organization's business and performance goals. The SRM provides guidance in risk-adjusted security/privacy protection and in the design and implementation of security controls. It is linked to the security domain. An example of an SRM artifact for this domain is a continuous monitoring plan, which describes the organization's process of monitoring and analyzing the security controls and reporting on their effectiveness.

Figure 2.7 illustrates the interactions among the reference models.

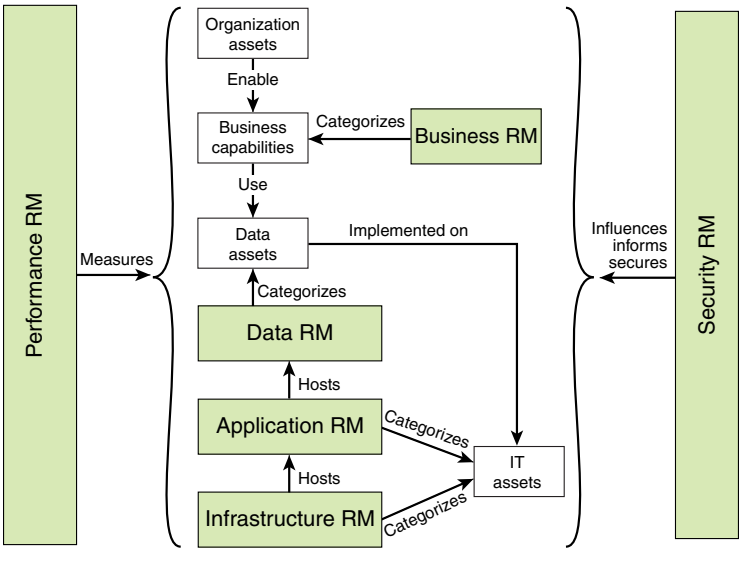


FIGURE 2.7 Relationships Between RM Components

https://t.me/learningnets

These reference models operate on four categories of assets:

- **Organization assets:** These assets include investments, programs, processes, applications, infrastructures, and individuals.
- **Business capabilities:** A business capability represents the ability of an organization to perform an activity that results in an outcome of value. A business capability can be viewed as an assembly of organization assets for a specific purpose.
- **Data assets:** Data assets include databases, files, and other data resources available to the organization.
- **IT assets:** IT assets include devices, peripherals, systems, applications, and IT capital investments.

Figure 2.8 shows in more detail the interaction between the security reference model and the other reference models.

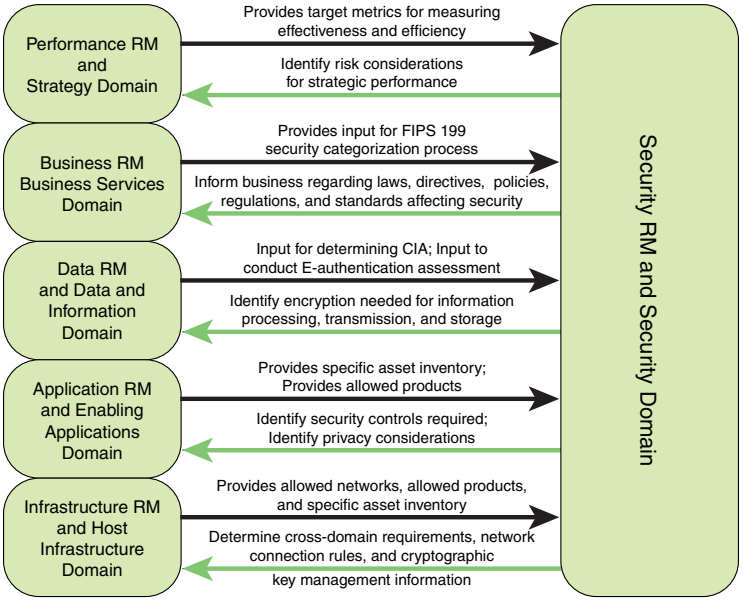


FIGURE 2.8 Interactions Between the Security Reference Model and Other Reference Models

An enterprise architecture is a powerful methodology for enabling enterprise and security governance, and it should be viewed as an essential element of governance.

https://t.me/learningnets

Policies and Guidance

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, defines an information security policy as an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. It is an essential component of security governance, providing a concrete expression of the security goals and objectives of the organization. The policies, together with guidance documents on the implementation of the policies, are put into practice through the appropriate selection of controls to mitigate identified risks. The policies and guidance need to cover information security roles and responsibilities, a baseline of required security controls, and guidelines for rules of behavior for all users of data and IT assets.

2.4 Security Governance Approach

Effective security governance requires the development and clear documentation of a framework, which is a structured approach for overseeing and managing risk for an enterprise. The implementation and ongoing use of the governance framework enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management.

Security Governance Framework

The definition, monitoring, and maintenance of a security governance framework entails a number of tasks:

- Appoint a single executive to be ultimately responsible for security governance, whose duties including implementing the framework and developing and monitoring an information security strategy and security assurance program. The framework needs to encompass all of the elements discussed in Section 2.3.
- Decide and communicate to top executives the objectives of the security governance framework, including ensuring alignment with overall organization policies and goals, enhancing business value, and adequately managing risk.
- Ensure integration of the security architecture with the enterprise architecture, as discussed in Section 2.3.
- Include a process that enables the governing body to evaluate the operation of the information security strategy to ensure that it aligns with business needs the organization's current risk appetite.
- Regularly review the organization's risk appetite to ensure that it is appropriate for the current environment in which the organization operates.
- Formally approve the information security strategy, policy, and architecture.

https://t.me/learningnets

Security Direction

A governing body is responsible for ensuring that there is effective security direction. Typically, the governing body consists of those individuals ultimately responsible for what the organization does. In a publicly held company, for example, this is the board of directors, supplemented by executive managers who have operational responsibility for various business units.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) recommends that effective security direction be provided by a combination of a single individual responsible for information security supported by a governing body. The single individual is a CISO or equivalent executive. This individual's responsibilities include implementing the organization's overall approach and ensuring that a security mind-set permeates the organization. This latter requirement entails coordination and collaboration with executives, managers, and operations personnel.

The SGP also recommends that the governing body include the CISO and have a mission to support the CISO as well as review the activities that are under the CISO's direction. Other members of the governing body could include the CIO, key department heads, and heads of business support functions such as human resources. The governing body assists in the coordination of security activities and ensuring that the CISO has the resources and authority required to effect needed changes. In addition, the governing body reports security status and plans to the stakeholders.

COBIT 5 provides a more elaborate governing body structure than the SGP suggests, and it is worthwhile for larger organizations. COBIT 5 distinguishes five distinct roles/structures:

- **Chief information security officer (CISO):** The CISO has overall responsibility for the enterprise information security program. The CISO is the liaison between executive management and the information security program. The CISO should also work with key business stakeholders to address information protection needs. The CISO is responsible for:
  - Establishing and maintaining an ISMS
  - Defining and managing an information security risk treatment plan
  - Monitoring and reviewing the ISMS
- **Information security steering (ISS) committee:** This committee ensures, through monitoring and review, that good practices in information security are applied effectively and consistently throughout the enterprise. The ISS committee is responsible for enterprisewide information security decision making in support of strategic decisions made by the enterprise risk management committee.

https://t.me/learningnets

- **Information security manager (ISM):** The ISM has overall responsibility for the management of information security efforts, including application security, infrastructure security, access management, threat and incident management, risk management, awareness program, metrics, and vendor assessments.
- **Enterprise risk management (ERM) committee:** This committee is responsible for the decision making of the enterprise to assess, control, optimize, finance, and monitor risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.
- **Information custodians/business owners:** These individuals serve as liaisons between the business and information security functions. They are associated with types of information, specific applications, or business units in an enterprise. They serve as trusted advisors and monitoring agents regarding information within the business.

COBIT 5 makes a distinction between the CISO and the ISM, with the CISO being a C-level position with oversight of an ISM, who has operational management responsibilities [ISAC08]. Other organizations combine the roles of CISO and ISM and may dispense with the CISO title.

Also, many organizations have a single security governing body, but COBIT 5 recommends a split into two committees for larger organizations. The ISS committee focuses on ensuring that security policies and practices are effectively implemented and monitored, and the ERM committee focuses on risk assessment. The suggested composition of the ISS committee is as follows:

- **CISO:** Serves as ISS committee chair and liaison to the ERM committee.
- **ISM:** Communicates design, implementation, and monitoring of practices.
- **Information custodians/business owners:** Are in charge of certain processes or business applications; responsible for communicating business initiatives that may impact information security and information security practices that may impact the user community.
- **IT manager:** Reports on the status of IT-related information security initiatives.
- **Representatives of specialist functions:** May include, permanently or as needed, representatives from internal audit, human resources, and legal departments.

The suggested composition of the ERM committee is as follows:

- **CISO:** Provides the committee with advice on specific information risks.
- **CEO, COO, CFO, etc.:** One or more representatives of senior executive management.

https://t.me/learningnets

- **Information custodians/business owner:** Are in charge of certain processes or business applications; responsible for communicating business initiatives that may impact information security and information security practices that may impact the user community.
- **Audit/compliance representative:** Advises committee on compliance risk.
- **Legal representative:** Provides legal input.
- **CRO:** Advises on risk from strategic, financial, operational, reputational, and compliance perspectives.

Responsible, Accountable, Consulted, and Informed (RACI) Charts

COBIT addresses the responsibility of all roles played by employees involved in IT governance actions. The COBIT responsibility model is formalized through a RACI chart matrix attached to all 34 COBIT processes. RACI explains what the responsibilities of all employees are regarding the key activities performance:

- **Responsible:** A person doing an activity and expected to deliver or submit the assigned work portion within the given deadlines. For example, in the case of software development project, developers are responsible.
- **Accountable:** A person with decision-making authority and who is expected to ensure the successful completion of project work. For example, a team leader or a project coordinator is accountable.
- **Consulted:** A stakeholder who should be included in any decision making or work activity by being consulted prior to the decision or action. This may a person whose area of responsibility would be affected by the activity, such as a business unit manager, or a person whose expertise should be consulted, such as a technical professional.
- **Informed:** A person who needs to know of decision making or actions after they occur. Such a person may have a direct concern in the outcome and progress of the work.

RACI charting helps avoid the following problems:

- Unclear accountability between individuals or departments
- Redundancies or work not being accomplished
- Delayed or incomplete work
- Inadequate communication and/or coordination
- Unclear approval/decision-making processes

https://t.me/learningnets

Table 2.4 shows a portion of the RACI chart for security governance. The table indicates which entity is accountable for each activity, and which entity or entities are responsible for that activity.

TABLE 2.4 Partial COBIT 5 RACI Chart for Organizational Structures

Activity	CISO	ISS	ISM	ERM	IC/BO
Identify and communicate information security threats, desirable behaviors, and changes needed to address these points.	**A**		**R**		
Ensure that environmental and facilities management adheres to information security requirements.	**A**		**R**		
Provide ways to improve efficiency and effectiveness of the information security function (for example, through training of information security staff; documentation of processes, technology, and applications; and standardization and automation of the process).	**A**		**R**		
Define and communicate an information security strategy that is in line with the business strategy.	**R**	**A**			
Research, define, and document information security requirements.	**R**	**A**			
Validate information security requirements with stakeholders, business sponsors, and technical implementation personnel.	**R**	**A**			
Develop information security policies and procedures.	**R**	**A**			
Define and implement risk evaluation and response strategies and cooperate with the risk office to manage the information risk.	**R**			**A**	
Ensure that the potential impact of changes is assessed.	**R**	**A**			
Collect and analyze performance and compliance data related to information security and information risk management.	**R**		**R**		
Raise the profile of the information security function within the enterprise and potentially outside the enterprise.		**R**			**R**

A = accountable

R = responsible

IC/BO = Information custodians/ business owners

https://t.me/learningnets

2.5 Security Governance Evaluation

An ancient Roman saying asks "Who will guard the guards themselves?" Those who are responsible for enterprise governance and information security governance need to be open to evaluation of their efforts at governance. In a publicly held corporation, the board performs or commissions such evaluation, and in any organization, the auditing function illustrated in Figure 2.7 encompasses an assessment of the governance function.

Johnston and Hale's article "Improved Security Through Information Security Governance" reports a useful set of metrics for evaluating security governance [JOHN09] (see Table 2.5).

TABLE 2.5 Indicators of Information Security Governance Effectiveness

Indicator Category	Indicators
Executive management support	Executive management understands the relevance of information security to the organization Executives promote effective information security governance Executives actively support the information security program Executives comply with all aspects of the information security program Executive management understands their responsibility for information security Executives understand the liability associated with not executing information security responsibilities
Business and information security relationship	Security investments are optimized to support business objectives Business process owners actively support the information security program Business process owners view security as an enabler Business process owners are involved in evaluating security alternatives Business process owners actively support the development of a security culture Business process owners accept responsibility for information security Business process owners are accountable for information security
Information protection	All information in use within the organization is identified Information is classified according to criticality Information is classified according to sensitivity Information classifications are enforced Information classifications are applied to information received from outside entities Information classifications are applied to information provided to an outside entity Ownership responsibilities for all information are assigned Applications that process sensitive information are identified Applications that support critical business processes are identified Data retention standards are defined and enforced

https://t.me/learningnets

The metrics fall into three categories:

- **Executive management support:** This is a critical component for cybersecurity program success. If top executives exhibit an understanding of security issues and take an active role in promoting security, this influence is felt throughout the firm. Strong executive management security awareness and support promotes a culture of secure practices.
- **Business and information security relationship:** An effective security governance program conveys a strong relationship between business goals and objectives and information security. When information security is incorporated into the enterprise planning process, employees tend to feel a greater responsibility for the security of their assets and view security not as an impediment but as an enabler.
- **Information protection:** These indicators of security governance effectiveness deal with the pervasiveness and strength of information security mechanisms. These indicators reflect the degree of awareness of information security issues and the level of preparedness, enterprisewide, to deal with attacks.

The SGP mandates that an organization adopt a consistent and structured approach to information risk management to provide assurance that information risk is adequately addressed. A key element is that a structured technique be used at the governing body level, such as the ISF Business Impact Reference Table (BIRT), discussed in Chapter 3. The BIRT is used to document the maximum level of risk or harm that the organization is prepared to accept in any given situation and is used to inform any decisions about information risk throughout the organization.

Based on the risk appetite, the security strategy, security controls, and security assessment measures are developed.

2.6 Security Governance Best Practices

The ISF SGP breaks down the best practices in the security governance category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Security governance approach:** This area provides guidance for establishing, maintaining, and monitoring an information security governance framework, which enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management.

https://t.me/learningnets

- **Security governance framework:** This topic provides a checklist of actions for establishing a security governance framework and ensuring that the organization's overall approach to information security supports high standards of governance.
- **Security direction:** This topic outlines a recommended top-down management structure and mechanism for coordinating security activity (for example, an information security program) and supporting the information security governance approach. It includes discussion of a CISO, a working group, and the tasks of each.

- **Security governance components:** This area provides guidance for supporting the information security governance framework by creating an information security strategy and implementing an information security assurance program that are aligned with the organization's strategic objectives.
  - **Information security strategy:** Provides a checklist for developing an information security strategy.
  - **Stakeholder value delivery:** Focuses on how the organization should implement processes to measure the value delivered by information security initiatives and report the results to all stakeholders.
  - **Information security assurance:** Discusses actions to assure that information risk is being adequately addressed.

2.7 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

architecture
C-level
chief executive officer (CEO)
chief information officer (CIO)
chief information security officer (CISO)
chief operating officer (COO)
chief privacy officer (CPO)
chief risk officer (CRO)
chief security officer (CSO)
enterprise architecture
enterprise risk management (ERM) committee
Federal Enterprise Architecture Framework (FEAF)
governance
information security architecture
information security governance
information security implementation/operations
information security steering (ISS) committee
information security management
information security strategic planning
information technology (IT)
IT strategic planning

https://t.me/learningnets

RACI chart
security governance
security implementation/ operations
security management
security program
stakeholder
strategic plan

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Briefly differentiate between information security governance and information security management.
2. Explain how the three supplemental factors in Figure 2.1—internal incident and global vulnerability reports, standards and best practices, and user feedback—play interconnected roles in designing a security program.
3. Differentiate between internal and external stakeholders from an information security point of view.
4. What are the two key pillars on which IT strategy planning should ideally be based?
5. What are the three categories of metrics for evaluating an organization's security governance?
6. What are the five roles within a security governing body structure defined in COBIT 5?
7. Explain the acronym RACI from context of information security policy.

2.8 References

BSA03: Business Software Alliance, *Information Security Governance: Toward a Framework for Action.* 2003. https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf

CGTF04: Corporate Governance Task Force, *Information Security Governance: A Call to Action.* U.S. Department of Homeland Security, 2004.

EAPA17: The EA Pad. *Basic Elements of Federal Enterprise Architecture.* https://eapad.dk/gov/us/common-approach/basic-elements-of-federal-enterprise-architecture/

HAYD08a: Haydamack, C., "Strategic Planning Processes for Information Technology," *BPTrends*, September 2008.

https://t.me/learningnets

HAYD08b: Haydamack, C., & Johnson, S., *Aligning IT with Business Goals Through Strategic Planning.* Intel Information Technology White Paper, December 2008.

ISAC08: ISACA, *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*. 2008. www.isaca.org

ITGI06: IT Governance Institute, *Information Security Governance Guidance for Boards of Directors and Executive Management*. 2006. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

JOHN09: Johnston, A., & Hale, R., "Improved Security Through Information Security Governance." *Communications of the ACM*, January 2009.

JUIZ15: Juiz, C., & Toomey, M., "To Govern IT, or Not to Govern IT?" *Communications of the ACM*, February 2015.

OHKI09: Ohki, E., et al., "Information Security Governance Framework." *First ACM Workshop on Information Security Governance (WISG)*, November 2009.

OMB13: Office of Management and Budget, *Federal Enterprise Architecture Framework.* 2013.

PETE12: Peters, C., & Schuman, B., *Achieving Intel's Strategic Goals with IT.* Intel Information Technology White Paper, February 2012.

SESS07: Sessions, R., "A Comparison of the Top Four Enterprise-Architecture Methodologies." *Microsoft Developer Network*, May 2007. http://www3.cis.gsu.edu/dtruex/courses/CIS8090/2013Articles/A%20Comparison%20of%20the%20Top%20Four%20Enterprise-Architecture%20Methodologies.html

SGM17: Strategic Management Group, *Strategic Planning Basics.* http://www.strategymanage.com/strategic-planning-basics/retrieved April 6, 2017.

TOG11: The Open Group, *The Open Group Architecture Framework (TOGAF).* 2011. http://www.opengroup.org/subjectareas/enterprise/togaf

ZIA15: Zia, T., "Organisations Capability and Aptitude Towards IT Security Governance." *2015 5th International Conference on IT Convergence and Security (ICITCS)*, August 2015.

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Chapter 3

Information Risk Assessment

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War*, Sun Tzu

Learning Objectives

After studying this chapter, you should be able to:

- Understand the methodology for asset identification for the various types of assets.
- Explain the STRIDE threat model.
- Present an overview of vulnerability identification techniques.
- Provide a comparison of quantitative and qualitative risk assessment.
- Explain the purpose and approach of Factor Analysis of Information Risk.
- Understand the key elements of risk analysis.
- Explain the major options for risk treatment.
- Present an overview of risk assessment best practices.

The ultimate objective of risk assessment is to enable organization executives to determine an appropriate budget for security and, within that budget, implement security controls to optimize the level of protection. This objective is met by providing an estimate of the potential cost to the organization of security breaches, coupled with an estimation of the likelihood of such breaches.

While the utility of risk assessment should be obvious, and indeed it must be considered essential, it is well at the outset to recognize its limitations, which are clearly summarized in *Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions* [MILL17]. If the scale of

https://t.me/learningnets

the effort is too ambitious, projects become large, complicated, and unreviewable, with a tendency to leave out things that are not easily quantified. On the other hand, if effective ways of calculating risk are not employed, managers tend to underestimate the magnitude of the risk and choose to invest in other areas that are understood better and lead to clear payoffs. Thus, responsible executives need to develop a plan for risk assessment that is balanced between too much and too little. Fortunately, relying on well-accepted best practices, such as those in the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP), makes it possible to develop a systematic approach that incorporates best practices that are reasonable for a given organization.

3.1 Risk Assessment Concepts

Risk assessment is a complex subject that is more art than science and calls for considerable management judgment. A good way to begin looking at risk assessment is to consider the terminology listed in Table 3.1, based largely on definitions in ISO 27005, *Information Security Risk Management System Implementation Guidance*. Nearly identical terminology is used in two other important documents: SP 800-30, *Guide for Conducting Risk Assessments*, and X.1055, *Risk Management and Risk Profile Guidelines for Telecommunication Organizations*.

TABLE 3.1 Information Security Risk Terminology

Term	ISO 27005 Definition
asset	Anything that has value to the organization and which therefore requires protection.
impact	Adverse change to the level of business objectives achieved. ISO 27005 uses the term **consequence** instead of impact. SP800-30 uses the terms **impact level** and **impact value** instead of impact.
event	Occurrence or change of a particular set of circumstances.
threat	Potential cause of an unwanted incident, which may result in harm to a system or an organization.
threat action	A realization of a threat—that is, an occurrence in which a vulnerability is exploited as a result of either an accidental event or an intentional act.
threat agent	A system entity that performs a threat action or an event that results in a threat action.

https://t.me/learningnets

Term	ISO 27005 Definition
vulnerability	A weakness of an asset or a control that can be exploited by one or more threats.
security incident	An adverse event whereby some aspect of security could be threatened.
risk	A combination of the consequences of an information security event and the associated likelihood of occurrence.
likelihood	The chance of something happening, especially the likelihood of a security incident. X.1055 uses the term **risk of exposure (RoE)** instead of likelihood.
level of risk	The magnitude of a risk, expressed in terms of the combination of consequences and their likelihood.
security control	The management, operational, and technical control countermeasures prescribed to protect the confidentiality, integrity, and availability or other security property of an asset.
residual risk	Risk remaining after risk treatment.
risk identification	The process of finding, recognizing, and describing risks.
risk analysis	The process of comprehending the nature of risk and determining the level of risk.
risk criteria	Terms of reference against which the significance of a risk is evaluated.
risk evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
risk assessment	The overall process of risk identification, risk analysis, and risk evaluation.
risk treatment	The process of modifying risk. SP800-30 uses the term **risk response** instead of risk treatment.
risk management	Coordinated activities to direct and control an organization with regard to risk.

Threats and vulnerabilities need to be considered together. A threat is the potential for a threat agent to intentionally or accidentally exploit a vulnerability, which is a weakness in a system's security procedures, design, implementation, or internal controls. A threat acting on a vulnerability produces a security violation, or breach. The level of risk is a measure that an organization can use in assessing the need for and the expected cost of taking remedial action in the form of risk treatment.

Figure 3.1 illustrates in general terms a universally accepted method for determining the level of risk.

https://t.me/learningnets

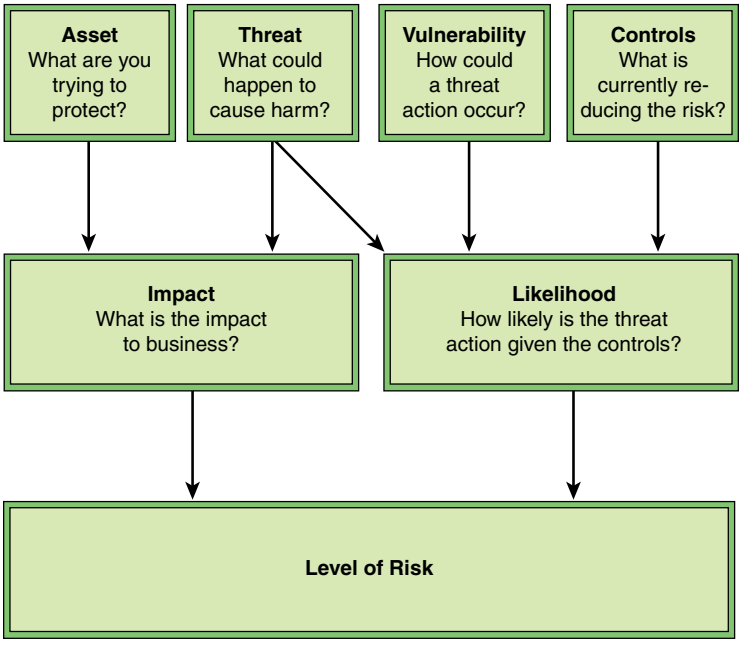


FIGURE 3.1 Determining Information Security Risk

Two main threads, impact and likelihood, should be pursued in parallel. An organization pursues the following tasks related to these threads:

- **Impact:** Consider these two elements in determining impact:
  - **Assets:** Develop an inventory of the organization's assets, which includes an itemization of the assets and an assigned value for each asset. These include intangible assets such as reputation and goodwill, as well as tangible assets, such as databases, equipment, business plans, and personnel.
  - **Threat:** For each asset, determine the possible threats that could reduce the value of that asset.

  Then, for each asset, determine the impact to the business, in terms of cost or lost value, of a threat action occurring.
- **Likelihood:** Consider the three elements in determining likelihood:
  - **Threat:** For each asset, determine which threats are relevant and need to be considered.

https://t.me/learningnets

- **Vulnerability:** For each threat to an asset, determine the level of vulnerability to the threat. That is, determine specifically for an asset how a threat action could be achieved.
- **Controls:** Determine what security controls are currently in place to reduce the risk.

Then determine how likely it is that a threat action will cause harm, based on the likelihood of a threat action and the effectiveness of the corresponding controls that are in place.

Finally, the level of risk is determined as the combination of the cost of the threat occurring combined with the likelihood of the threat occurring.

For example, a hacker (threat agent) may exploit known vulnerabilities (vulnerability) in a remote authentication protocol (vulnerability target) to disrupt (policy violated) remote authentication (asset exposed). The threat is unauthorized access. The assets are anything that can be compromised by an unauthorized access. The vulnerability expresses how a threat action could occur (for example, by access through a web interface). Existing security controls for this vulnerability reduce the likelihood of a threat action.

Note that both factors, impact and likelihood, are necessary in determining a budget allocation for security controls. If an organization focuses only on impact, the inclination will be to invest much of the security budget on high-impact threats, even if the likelihood of the impact is extremely small. Thus, threats that produce a low or moderate impact and are realized frequently may be given little attention, with the net effect of the overall loss to the business being higher than needed. Conversely, an organization errs in allocating security funds on the basis of likelihood alone. If a relatively rare security event that has very high impact costs is ignored, the organization is exposed to a very high security loss.

Risk Assessment Challenges

An organization faces enormous challenges in determining the level of risk. In general terms, these challenges fall into two categories: the difficulty of estimating and the difficulty of predicting. Consider first the problem of estimation of each of the four elements that contribute to determining risk:

- **Asset:** An organization needs to put a value on individual assets and how that value may be reduced by a specific threat—in other words, the impact value. A single example indicates how difficult this is. If a company maintains a database of customer credit card numbers, what is the impact of the theft of that database? There are potential legal fees and civil penalties, loss of reputation,

https://t.me/learningnets

loss of customers, and lowering of employee morale. Assessing the magnitude of these costs is a formidable undertaking.

- **Threat:** In determining the threats facing an organization, there is past experience to go on and, as discussed subsequently, numerous publicly available reports list current threats and their corresponding frequencies. Even so, it should be clear that it is difficult to determine the entire range of threats that are faced as well as the likelihood of any threat being realized.
- **Vulnerability:** An organization may face security vulnerabilities that it is not aware of. For example, software vendors have been known to delay revealing a security vulnerability until a patch is available or even delaying releasing a patch to a portion of a vulnerability until a complete patch is available (see, for example, [ASHO17], [KEIZ17]). Further, a patch may introduce new vulnerabilities. As another example, a company may have a fireproof barrier constructed around a data center enclosure. But if the contractor does not install a barrier that meets the specification, there may be no way for the company to know this.
- **Controls:** Controls are implemented to reduce vulnerability and therefore reduce the likelihood of particular threats being realized. However, it may be very difficult to assess the effectiveness of given controls, including software, hardware, and personnel training. For example, a particular threat action may be relatively unlikely, but controls may be introduced because of the high impact in the event that the threat action succeeds. But if the event rarely occurs, the organization has difficulty in determining whether the control has the desired effect. The threat action may be artificially generated to test the system, but this artificial action may not be realistic enough to get a true picture of how effective a control is.

Another challenge in risk assessment is the difficulty of predicting future conditions. Again, considering the four elements, the following problems emerge.

- **Asset:** Whether the planning period is one year, three years, or five years, changes in the value of an organization's assets complicate the effort to estimate the impact of a security threat. Company expansion, software or hardware upgrades, relocation, and a host of other factors may come into play.
- **Threat:** It is difficult at best to assess the current threat capability and intentions of potential adversaries. Future projections are even more subject to uncertainty. Entire new types of attack may emerge in a very short period of time. And, of course, without complete knowledge of the threat, it is impossible to provide a precise assessment of impact.

https://t.me/learningnets

- **Vulnerability:** Changes within the organization or its IT assets may create unexpected vulnerabilities. For example, if an organization migrates a substantial portion of its data assets to a cloud service provider, the degree of vulnerability of that provider may not be known to the organization with a high level of confidence.
- **Controls:** New technologies, software techniques, or networking protocols may provide opportunities for strengthening an organization's defenses. But it is difficult to predict the nature of these new opportunities, much less their cost, and so resource allocation over the planning period may not be optimal.

Complicating matters is the many-to-many relationship between threats, vulnerabilities, and controls. A given threat may be able to exploit multiple vulnerabilities, and a given vulnerability may be subject to attack by multiple threats. Similarly, a single control may address multiple vulnerabilities, and a single vulnerability may require the implementation of multiple controls. These facts complicate the planning of what controls to select and how much of the budget to allocate for various forms of mitigation.

With all these challenges, it is clear that today's executives are unable to follow the advice of Sun Tzu of ignoring the risk by making the position unassailable. Responsible executives can, however, follow a systematic methodology of risk assessment based on well-established best practices.

Risk Management

Risk assessment is one part of the broader security task of risk management. National Institute of Standards and Technology (NIST) Cybersecurity SP 800-37, *Risk Management Framework for Information Systems and Organizations*, states that risk management includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring. It also includes enterprise-level activities to help better prepare organizations to execute a risk management framework at the system level.

To place risk assessment into the context of risk management, this subsection summarizes two risk management concepts defined by ITU-T and ISO.

X.1055 Risk Management Process

Risk management is an iterative process, as illustrated in Figure 3.2, based on one in X.1055.

https://t.me/learningnets

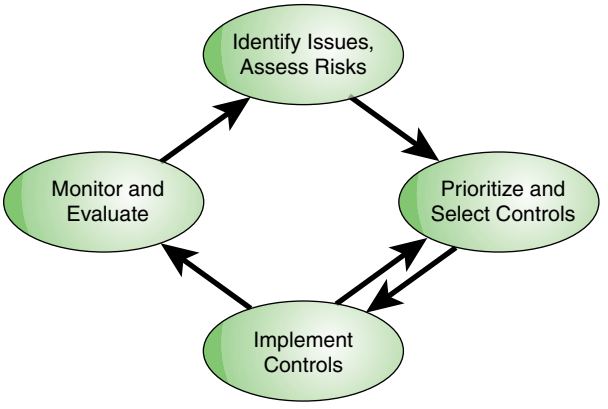


FIGURE 3.2 Risk Management Life Cycle

The steps are as follows:

1. Assess risk based on assets, threats, vulnerabilities, and existing controls. From these inputs, determine impact and likelihood and then the level of risk.
2. Identify potential security controls to reduce risk and prioritize the use of these controls.
3. Allocate resources, roles, and responsibilities and implement controls.
4. Monitor and evaluate risk treatment effectiveness.

The results of the final step are fed back into the next iteration of the risk management life cycle.

ISO 27005, Information Security Risk Management

While a simple risk analysis worksheet may be suitable for smaller organizations, for larger organizations, a broader framework to guide risk assessment is advisable. The most important such framework is ISO 27005, which describes a systematic approach to managing information security risk, particularly in the context of ISO 27001, *ISMS Requirements*.

Figure 3.3 shows the overall risk management process defined in ISO 27005.

https://t.me/learningnets

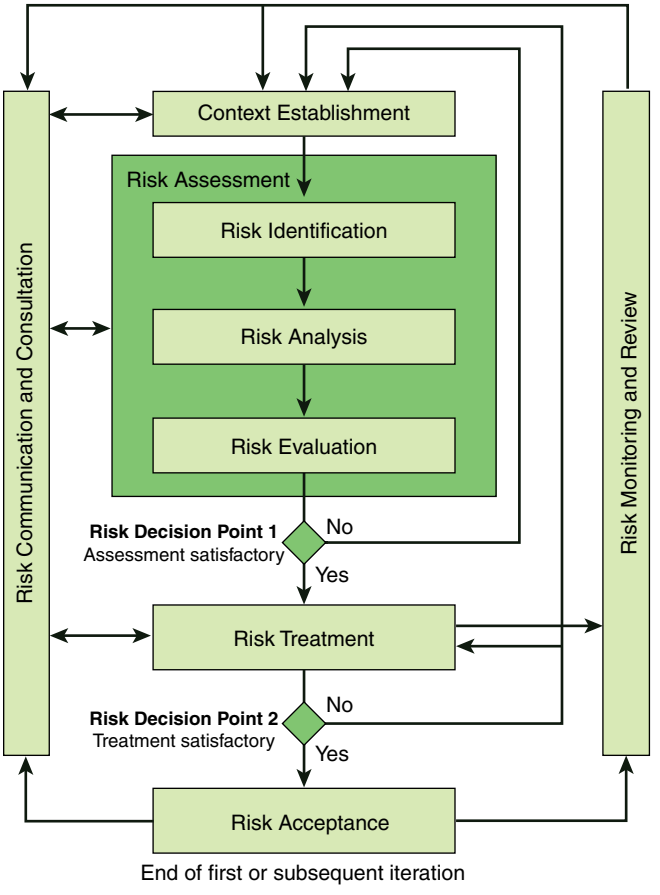


FIGURE 3.3 ISO 27005 Risk Management Process

This process consists of a number of separate activities:

- **Context establishment:** This is a management function that involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organizational structure for information security risk management. Risk criteria are based on organizational objectives and external and internal context. They can be derived from standards, laws, policies, and other requirements. Table 3.2 lists the guidelines provided in ISO 27005 for context establishment.

https://t.me/learningnets

TABLE 3.2 ISO 27005 Risk Management Context Establishment

Category	Consideration or Criteria
Purpose of risk management	■ Legal compliance and evidence of due diligence ■ Preparation of a business continuity plan ■ Preparation of an incident response plan ■ Description of the information security requirements for a product, a service or a mechanism
Risk evaluation criteria	■ The strategic value of the business information process ■ The criticality of the information assets involved ■ Legal and regulatory requirements and contractual obligations ■ Operational and business importance of availability, confidentiality, and integrity ■ Stakeholder expectations and perceptions and negative consequences for goodwill and reputation
Impact criteria	■ Level of classification of the impacted information asset ■ Breaches of information security (for example, loss of confidentiality, integrity, and availability) ■ Impaired operations (internal or third parties) ■ Loss of business and financial value ■ Disruption of plans and deadlines ■ Damage of reputation ■ Breaches of legal, regulatory, or contractual requirements
Risk acceptance criteria	■ May include multiple thresholds, with a desired target level of risk but provision for senior managers to accept risks above this level under defined circumstances ■ May be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk ■ Different criteria may apply to different classes of risk (for example risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement) ■ May include requirements for future additional treatment (for example a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period)

- **Risk assessment:** ISO 27001 defines risk assessment as consisting of three activities:
  - **Risk identification:** Involves the identification of risk sources, events, their causes, and their potential consequences. It involves historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

https://t.me/learningnets

- **Risk analysis:** Provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation.
- **Risk evaluation:** Assists in the decision about risk treatment by comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.

- **Risk treatment:** Involves the following:
  - Avoiding the risk by deciding not to start or continue with an activity that gives rise to the risk
  - Taking or increasing risk in order to pursue an opportunity
  - Removing the risk source
  - Changing the likelihood
  - Changing the consequences
  - Sharing the risk with another party or parties (including contracts and risk financing)
  - Retaining the risk by informed choice
- **Risk acceptance:** Involves ensuring that residual risks are explicitly accepted by the managers of the organization.
- **Risk communication and consultation:** Encompasses the continual and iterative processes that an organization conducts to provide, share, or obtain information and to engage in dialogue with stakeholders regarding the management of risk.
- **Risk monitoring and review:** Includes ongoing monitoring and review of all risk information obtained from the risk management activities.

virtual machine
One instance of an operating system along with one or more applications running in an isolated partition within the computer. A virtual machine enables different operating systems to run in the same computer at the same time and also prevents applications from interfering with each other.

As shown, the risk management process is an iterative process. As mentioned earlier in this chapter, there are continual changes in business asset valuation, threat capability and frequency, vulnerability magnitude, and control technologies and techniques. In addition, implemented controls may not realize the anticipated benefits. Thus, the assessment and treatment of risk must be an ongoing activity.

Structure of This Chapter

The remainder of this chapter covers the topics introduced in this section. Sections 3.2 through 3.5 cover the four inputs to the risk assessment process indicated in Figure 3.1: assets, threats, controls, and vulnerabilities. Section 3.6 provides a general discussion

https://t.me/learningnets

of risk assessment approaches. Sections 3.7 through 3.9 discuss the lower three boxes in Figure 3.1: likelihood determination, impact assessment, and risk determination.

Sections 3.10 and 3.11 examine two key tasks depicted in Figure 3.3: risk evaluation and risk treatment.

3.2 Asset Identification

Risk identification is the identification of the assets, threats, existing controls, vulnerabilities, and impacts relevant to the organization and that serve as inputs to risk analysis. This section looks at asset identification.

A first step in risk assessment is to document and determine values for the organization's assets. An asset is anything of value to the business that requires protection, including hardware, software, information, and business assets. Many assets of various types can be identified, and the challenge is to develop a uniform way of documenting the assets, the security implications of each, and the costs associated with security incidents related to each. Asset valuation relates directly to business needs. Accordingly, the input for asset valuation needs to be provided by owners and custodians of assets, not by members of the risk assessment team.

Hardware Assets

Hardware assets include servers, workstations, laptops, mobile devices, removable media, networking and telecommunications equipment, and peripheral equipment. Key concerns are loss of a device, through theft or damage, and lack of availability of the device for an extended period. Another concern is device malfunction, due to deliberate malfunction or other causes. Asset valuation needs to take into account the replacement cost of the hardware, disruption losses, and recovery expenses.

Software Assets

Software assets include applications, operating systems and other system software, **virtual machine** and **container virtualization** software, software for **software-defined networking (SDN)** and **network function virtualization (NFV),** database management systems, file systems, and client and server software. Availability is a key consideration here, and asset valuation must take account of disruption losses and recovery expenses.

container virtualization
A technique in which the underlying operating environment of an application is virtualized. This is commonly the operating system kernel, and the result is an isolated container in which the application can run.

software-defined networking (SDN)
An approach to designing, building, and operating large-scale networks based on programming the forwarding decisions in routers and switches via software from a central server. SDN differs from traditional networking, which requires configuring each device separately and which relies on protocols that cannot be altered.

network function virtualization (NFV)
Virtualization of network functions which involves implementing these functions in software and running them on virtual machines.

https://t.me/learningnets

Information Assets

Information assets comprise the information stored in databases and file systems, both on-premises and remotely in the cloud. As an example, ITU-T X.1055 lists the following as types of information assets in a telecommunications or network environment:

- Communication data
- Routing information
- Subscriber information
- Blacklist information
- Registered service information
- Operational information
- Trouble information
- Configuration information
- Customer information
- Billing information
- Customer calling patterns
- Customer geographic locations
- Traffic statistical information
- Contracts and agreements
- System documentation
- Research information
- User manuals
- Training materials
- Operational or support procedures
- Business continuity plans
- Emergency plan fallback arrangements
- Audit trails and archived information

Asset valuation needs to take into account the impact of threats to confidentiality, privacy, integrity, and authenticity. As an example of questions involved in information asset evaluation, NISTIR 7621, *Small Business Information Security: The Fundamentals*, suggests the following:

- What would happen to my business if this information were made public?
- What would happen to my business if this information were incorrect?
- What would happen to my business if my customers or I couldn't access this information?

Table 3.3, from NISTIR 7621, is an example of a worksheet for recording this information, including a worked example.

https://t.me/learningnets

TABLE 3.3 Identify and Prioritize Information Types

	Example: Customer Contact Information	Info Type 1	Info Type 2	...
Cost of revelation (Confidentiality)	Medium			
Cost to verify information (Integrity)	High			
Cost of lost access (Availability)	High			
Cost of lost work	High			
Fines, penalties, customer notification	Medium			
Other legal costs	Low			
Reputation/public relations costs	High			
Cost to identify and repair problem	High			
Overall Score:	High			

Business Assets

The business assets category includes organization assets that don't fit into the other categories, including human resources, business processes, and physical plant. This category also includes intangible assets, such as organization control, know-how, reputation, and image of the organization.

Asset Register

In order to effectively protect assets, an organization needs to provide a systematic method of documenting assets and their security implications. This is done in an asset register that documents important security-related information for each asset. Examples of items that may be included for each asset are as follows:

- **Asset name/description:** This information uniquely identifies an asset.
- **Asset type:** This denotes the type of asset it is, such as physical/infrastructure assets, software, information, service, or human resource.
- **Asset class:** For purposes of risk assessment, an organization should group assets into classes so risks are measured against classes of assets rather than against individual assets. Asset class examples include desktops/workstations, servers, Payment Card Industry (PCI) devices, restricted/sensitive file shares, and restricted printers.

https://t.me/learningnets

- **Information assets:** An information asset defines specifically what kind of information is processed, transmitted, or stored by the asset (for example, customer personally identifiable information [PII], PCI data). This item does not apply to all assets.
- **Asset owner:** An organization should define the department/company function that owns an asset and is responsible for risk associated with the asset. This is also sometimes referred to as the risk owner or business owner.
- **Asset custodian:** This is the individual responsible for maintaining, monitoring, and managing the asset. This is typically a network or systems administrator.
- **Location:** This is the physical location of the asset.
- **Function/business process:** This is the business process or function the asset supports (for example, information processing facility).
- **Data type/classification:** The company's established information classification policy should be used to classify the information transmitted, processed, or stored by the asset. This helps drive the risk assessment later.
- **Asset value classification:** This could be a monetary value but more typically is a ranking, such as low, medium, or high.
- **Disaster recovery priority:** In the event of a security breach that affects multiple assets, this is the relative priority for devoting resources to recovery. This could be a numeric scale (for example, 1 to 10) or a low/medium/high scale.
- **Exposure level:** This is the degree to which an asset is exposed to threats. This depends, at least, on how the asset is shared and also may depend on other factors.

Table 3.4, from the ISACA document "Security Risk Management" [RITC13], is a simplified example of the type of elements that should go into an asset register.

TABLE 3.4 Example Asset Register

Asset Name/ Description	Asset Classification	Disaster Recovery Priority	Description	Exposure Level
Personnel	High	1	Employees	Medium
Client PII	High	1	Personally identifiable information	Low
Production web server	Medium	1	Company primary website (no sensitive data)	High

https://t.me/learningnets

3.3 Threat Identification

Threat identification is the process of identifying threat sources with the potential to harm system assets. Threat sources are categorized into three areas:

- **Environmental:** Examples include floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and power failure.
- **Business resources:** Examples include equipment failure, supply chain disruption, and unintentional harm caused by employees.
- **Hostile actors:** Examples include hackers, hacktivists, insider threats, criminals, and nation-state actors.

Both environmental and business resource threats must be recognized and addressed, but the bulk of the effort of threat identification—and indeed of risk assessment and risk management—involves dealing with threats from hostile actors. That is the focus of this section.

The STRIDE Threat Model

STRIDE is a threat classification system developed by Microsoft that is a useful way of categorizing attacks that arise from deliberate actions [HERN06]. It involves the following categories:

- **Spoofing identity:** An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password. Security controls to counter such threats are in the area of *authentication*.
- **Tampering with data:** Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and alteration of data as it flows between two computers over an open network, such as the Internet. Relevant security controls are in the area of *integrity*.
- **Repudiation:** Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise (for example, a user performing an illegal operation in a system that lacks the ability to trace the prohibited operations). Relevant security controls are in the area of *non-repudiation*, which refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user received the package.

https://t.me/learningnets

- **Information disclosure:** Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it (for example, the ability of users to read a file that they were not granted access to or the ability of an intruder to read data in transit between two computers). Relevant security controls are in the area of *confidentiality*.
- **Denial of service:** Denial-of-service (DoS) attacks deny service to valid users—for example, by making a web server temporarily unavailable or unusable. Relevant security controls are in the area of *availability*.
- **Elevation of privilege:** In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself—a dangerous situation indeed. Relevant security controls are in the area of *authorization*.

Threat Types

Many efforts have been made to categorize types of threats, and there is considerable overlap in the definition of some common terms. A large category of threat is malicious software, or *malware*, which is a general term encompassing many types of software threats, including the following:

- **Malware:** Malicious software. This is a general term encompassing many types of threats, including the ones listed here.
- **Virus:** Malware that, when executed, tries to replicate itself into other executable code; when it succeeds, the code is said to be *infected*. When the infected code is executed, the virus also executes.
- **Worm:** A computer program that runs independently and propagates a complete working version of itself onto other hosts on a network.
- **Ransomware:** A type of malware that tries to extract a ransom payment in exchange for unblocking access to an asset that belongs to the victim or in exchange for a promise not to release the data captured by the ransomware.
- **Spam:** The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- **Logic bomb:** A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.

https://t.me/learningnets

- **Trojan horse:** A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
- **Backdoor (trapdoor):** Any mechanisms that bypass a normal security check; it may allow unauthorized access to functionality.
- **Mobile code:** Software (for example, scripts, macros, or other portable instructions) that are shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
- **Exploit:** Code specific to a single vulnerability or set of vulnerabilities.
- **Exploit kit:** Prepackaged software made available for use by others that uses an arsenal of exploits to infect a computer. Then it typically installs malware.
- **Downloader:** A program that installs other items on a machine that is under attack. Usually, a downloader is sent in an email.
- **Dropper:** An installer that surreptitiously carries malware to be executed on the compromised machine. Droppers are often disguised and hidden in a computer's directories, so that although they are visible, they look like valid programs or file types.
- **Auto-rooter:** A malicious hacker tool used to break into new machines remotely.
- **Kit (virus generator):** A set of tools for generating new viruses automatically.
- **Spammer program:** A program that is used to send large volumes of unwanted email.
- **Flooder:** A program that is used to attack networked computer systems with a large volume of traffic to carry out a DoS attack.
- **Keyloggers:** Software that captures keystrokes on a compromised system.
- **Rootkit:** A set of hacker tools used after an attacker has broken into a computer system and gained root-level access.
- **Zombie or bot:** A program activated on an infected machine that launches attacks on other machines.
- **Spyware:** Software that collects information from a computer and transmits it to another system.
- **Adware:** Advertising that is integrated into software. It results in pop-up ads or redirection of a browser to a commercial site.

https://t.me/learningnets

Other cybersecurity threat terms frequently encountered include the following:

- **Remote access attacks:** Attacks made across the Internet or a corporate network.
- **Denial-of-service (DoS) attack:** An attack that prevents authorized access to resources or the delaying of time-critical operations.
- **Distributed denial-of-service (DDoS) attack:** A DoS technique that uses numerous hosts to perform the attack.
- **DNS attacks:** Attacks that encompass a variety of exploits that subvert the functioning of the Domain Name System (DNS), which provides a mapping between hostnames and IP addresses.
- **Hacker or cracker:** An unauthorized user who attempts to or gains access to an information system. Sometimes a distinction is made between individuals who are essentially harmless and just curious (hacker) and individuals who break security on a system for malign purposes (cracker); in other case these two terms are considered equivalent.
- **Injection flaw:** A vulnerability that is created from insecure coding techniques and results in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system.
- **Code injection:** Insertion of malicious code by exploiting an injection flaw.
- **Social engineering:** A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.
- **Phishing:** A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake website that requests information.
- **Password attack:** A method of accessing an obstructed device, using one of various methods, by capturing the user ID/password of a validated user.
- **Website exploit:** An attack that inserts malicious code on a web server, either to attack the server itself or as a means of attacking source systems of users who access the website.

These lists are not exhaustive but give you an idea of the scale of the challenge organizations face.

Sources of Information

Information on environmental threats is typically available from a variety of government and trade groups. Threats related to business resources are less easily documented but

https://t.me/learningnets

still generally can be predicted with reasonable accuracy. It is difficult to get reliable information on past events and to assess future trends for a variety of reasons, including the following:

- Organizations are often reluctant to report security events in an effort to save corporate image, avoid liability costs, and, in the case of responsible management and security personnel, avoid career damage.
- Some attacks may be carried out or at least attempted without being detected by the victim until much later, if ever.
- Threats continue to evolve as adversaries adapt to new security controls and discover new techniques.

Thus, keeping informed on threats is an ongoing and never-ending battle. The following discussion examines three important categories of threat information sources: in-house experience, security alert services, and global threat surveys.

An important source of information on threats is the experience an organization has already had in identifying attempted and successful attacks on its assets. An organization can obtain this information through an effective security monitoring and improvement function, as discussed in Chapter 18, "Security Monitoring and Improvement." However, this information is of more value for threat and incident management, described in Chapter 15, "Threat and Incident Management," "than for risk assessment. That is, detected attacks should prompt immediate remedial action rather than be folded into long-range actions.

Security alert services are concerned with detecting threats as they develop to enable organizations to patch code, change practices, or otherwise react to prevent a threat from being realized. Again, this category of information is of more value for threat and incident management, and these sources are addressed in Chapter 15.

Of great value for threat identification is the various global threat surveys that are readily available. The most important global threat survey are examined in this section.

Verizon Data Breach Investigations Report

Perhaps the most important source of information that an organization can consult is the annual Verizon Data Breach Investigations Report (DBIR). This authoritative and highly respected report is based on data on security incidents systematically collected from a wide variety of organizations. The results in the 2018 report are based on data from more than 53,000 security incidents and over 2,200 data compromises from 65 countries and 67 organizations. The results are broken down by 20 industry sectors,

https://t.me/learningnets



Data Breach Investigations Report
http://www.verizonenterprise.com/verizon-insights-lab/dbir/

such as accommodation, entertainment, finance, healthcare, manufacturing, public, and utilities. Further, threats are broken down along three dimensions:

- **Pattern:** This includes DoS, privilege misuse, lost and stolen assets, point of sale, miscellaneous errors, web app attacks, crimeware, payment care skimmers, and cyber-espionage.
- **Action:** This includes hacking, malware, social breach, error, misuse, physical breach, and environmental-based damage.
- **Asset:** This includes servers, media, user devices, persons, networks, kiosks/terminals, and embedded devices (for example, Internet of Things [IoT] devices).

Along each dimension, the number of security incidents and breaches are reported for each industry sector. The DBIR defines a *security incident* as a security event that compromises the integrity, confidentiality, or availability of an information asset. It defines a *breach* as an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party. The report also summarizes, with data, key aspects of the attack, including the following:

- **Actors:** Broken down into the categories outsiders, internal actors, state-affiliated actors, multiple parties, partners, and organized criminal groups.
- **Tactics:** Includes hacking, malware, leveraging stolen and/or weak passwords, social attacks, errors, privilege misuse, and physical actions.
- **Other common factors:** Includes malware installed via malicious email attachments, financially motivated breaches, related to espionage, and discovered by third parties.

Other more detailed breakdowns of types of attacks are included in DBIR. With this wealth of high-quality data, the DBIR is an essential tool in the threat identification process.



ISF Threat Horizon Report
https://www.securityforum.org/research/threat-horizon-2on-deterioration/

Threat Horizon Report

A useful complement to the DBIR is the annual Threat Horizon Report from the ISF. It differs from the DBIR in two ways. First, it is a more broad-brush treatment, identifying key threat trends rather than detailed threats and detailed target profiles. Second, the Threat Horizon Report attempts to project the likely major threats over the next two years.

The latest report, *Threat Horizon 2019*, highlights nine major threats, broken down into three challenging themes, that organizations can expect to face over the next two

https://t.me/learningnets

years as a result of increasing developments in technology. These are the key themes and challenges in the latest report are:

- **Disruption:** Disruption is likely due to an over-reliance on fragile connectivity requiring a seismic shift in the way business continuity is planned, practiced, and implemented. The major threats are:
  - Premeditated Internet outages bringing trade to its knees
  - Ransomware hijacks on the IoT
  - Privileged insiders being coerced into giving up the crown jewels
- **Distortion:** As trust in the integrity of information is lost, the monitoring of access and changes to sensitive information become critical, as does the development of complex incident management procedures. The major threats are:
  - Automated misinformation gaining instant credibility
  - Falsified information compromising performance
  - Subverted **blockchains** shattering trust
- **Deterioration:** Controls may be eroded by regulations and technology bringing a heightened focus on risk assessment and management in light of regulatory changes and the increased prevalence of artificial intelligence in everyday technology. The major threats are:
  - Surveillance laws exposing corporate secrets
  - Privacy regulations impeding the monitoring of insider threats
  - A headlong rush to deploy artificial intelligence (AI) leading to unexpected outcomes

blockchain
A data structure that makes it possible to create a digital ledger of transactions and share it among a distributed network of computers. Blockchain technology includes protocols and formats that provide for the secure update of and access to the ledger.

The Threat Horizon Report includes detailed recommendations for countering each threat. The report states that many of the recommendations can be quickly and easily implemented over the next two years.

ENISA Threat Landscape Report

Another very useful source of information is several threat documents from European Union Agency for Network and Information Security (ENISA). One of these is the *ENISA Threat Taxonomy* (2016), which provides a very detailed breakdown of potential cybersecurity threats. It is organized into a three-level hierarchy of high-level threats, threats, and threat details, and defines dozens of individual threat categories. It provides is a useful checklist for ensuring that an organization considers the full range of threats.

https://t.me/learningnets

kill chain
A systematic process used to target and engage an adversary to create desired effects. In the context of cybersecurity, it consists of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action.

A useful source of information on current threats is the *ENISA Threat Landscape Report*, most recently published in January 2018 [ENIS18]. Table 3.5 summarizes the results of the report. The 15 threats are ranked according to the volume of security incidents surveyed, and the Trend column refers to the relative change in the severity of consequences from each threat. For each threat, the report provides a **kill chain** for each specific threat, which defines the phases of a cyber attack.

TABLE 3.5 Top Cybersecurity Threats Reported by ENISA

Threat	Trend
1. Malware	Stable
2. Web-based attacks	Increasing
3. Web application attacks	Increasing
4. Phishing	Increasing
5. Spam	Increasing
6. DoS attacks	Increasing
7. Ransomware	Increasing
8. Botnets	Increasing
9. Insider threats (malicious, accidental)	Stable
10. Physical manipulation/damage/theft/loss	Stable
11. Data breaches	Increasing
12. Identity theft	Increasing
13. Information leakage	Increasing
14. Exploit kits	Declining
15. Cyber espionage	Increasing

The phases of the kill chain are as follows [MYER13, ENGE14]:

- **Reconnaissance:** The adversary determines likely targets for attack. This includes determining what information is available for targeting as well as what means are promising for targeting. For example, if names and contact details of employees are online, these could be used for social engineering purposes (for example, getting people to divulge usernames or passwords).
- **Weaponization:** The adversary couples an exploit with a means of gaining access to the specific system to be attacked. The result is a malicious payload, which is constructed on the attacker side, without access to the victim's system.
- **Delivery:** Weaponized payload is delivered to the victim via email, web access, USB, or other means.
- **Exploit:** The delivered bundle exploits a vulnerability to enable installation. This is relevant only when the attacker uses an exploit.

https://t.me/learningnets

- **Installation:** The malware package is installed on the asset. This step is relevant only if malware is part of the threat.
- **Command and control:** Once a threat is in an organization's system, the attacker creates a command and control channel to be able to operate the malware remotely.
- **Actions:** With command and control in place, the threat can be activated to achieve the goals of the attack, which could be to obtain data, do damage, or make a ransom demand.

The kill chain is useful for selecting security controls to counter a particular threat. However, as [ENGE14] points out, the kill chain focuses mostly on intrusion prevention, and only the last step is relevant to intrusion detection and recovery. Thus kill chain analysis needs to be balanced with other threat intelligence.



European Union Agency for Network and Information Security https://www.enisa.europa.eu



Trustwave Global Security Report https://www.trustwave.com/Resources/Global-Security-Report-Archive/

Trustwave Global Security Report

The Trustwave Global Security Report is a well-regarded annual survey of the cyberthreat landscape. The report is based on findings from extensive data sources, including breach investigations, global threat intelligence, product telemetry, and a number of research sources. Trustwave operates a number of **security operations centers (SOCs)** as a managed security service and from them has logged billions of security and compliance events each day, examined data from tens of millions of network vulnerability scans, and conducted thousands of penetration tests. Its infographic style makes the Trustwave Global Security Report easy to follow, yet it contains an extraordinary amount of detailed information that can assist in threat assessment and risk treatment [RUBE14]. The key features include the following:

security operations center (SOC)

A facility that tracks and integrates multiple security inputs, ascertains risk, determines the targets of an attack, contains the impact of an attack, and recommends and/or executes responses appropriate to any given attack. In some cases, an organization establishes a SOC for itself. In other cases, SOC services are outsourced to a private company that specializes in providing such services.

- Breakdown by type of data or other asset targeted, such as credit card data
- Median time between intrusion and detection
- Breakdown by vulnerability and exploitation, such as zero-day attacks on Adobe Flash Player, RIG exploit kit originating from malicious advertisements, and web attacks targeting WordPress
- Breakdown by method of intrusion, including remote access, SQL injection, misconfiguration, file upload, phishing/social engineering, malicious insider, code injection, and weak passwords

The report also provides a detailed breakdown of how various attacks are carried out and provides examples of existing malware currently operating. It also looks at the specific state of security in the areas of network, database, and application security. The report is detailed enough to provide specific guidance to security planners and managers.

https://t.me/learningnets



Cisco Annual Cybersecurity Report
http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

Cisco Annual Cybersecurity Report

The Cisco Annual Cybersecurity Report is yet another excellent source of threat information. The report is approximately organized along the lines of kill chain concepts. The report provides a detailed description of current attacker behavior patterns and also highlights coming vulnerabilities.

Fortinet Threat Landscape Report

The findings in the Fortinet Threat Landscape Report represent the collective intelligence of FortiGuard Labs, drawn from Fortinet's vast array of network devices/sensors within production environments. This comprises billions of threat events and incidents observed in live production environments around the world, reported quarterly. Three measures are reported:



Fortinet Threat Landscape Report
https://fortinet.com/fortiguard/threat-intelligence/threat-landscape.html

- **Volume:** Measure of overall frequency or proportion; the total number or percentage of observations of a threat event.
- **Prevalence:** Measure of spread or pervasiveness across groups; the percentage of reporting organizations that observed the threat event at least once.
- **Intensity:** Measure of daily volume or frequency; the average number of observations of a threat event per organization per day.

The detailed results are reported in aggregate and also broken down by region and by industry.

3.4 Control Identification

Controls for cybersecurity include any process, policy, procedure, guideline, practice, or organizational structure that modifies information security risk. Controls are administrative, technical, management, or legal in nature. Control identification is defined in ISO 27005 as the process of identifying existing and planned security controls, and suggests the following steps:

1. Review documents containing information about the controls (for example, risk treatment implementation plans). If the processes of information security management are well documented, all existing or planned controls and the status of their implementation should be available.
2. Check with the people with responsibility related to information security (e.g., security manager, building manager, and operations manager) and the users about which controls are really implemented for the information process or information system under consideration.

https://t.me/learningnets

3. Conduct an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented to determine whether they are working correctly and effectively.
4. Review results of audits.

This section provides a brief overview of the types of controls that may be contemplated. Details of these and other controls are provided in the appropriate chapters of this book. There are several particularly useful sources of information on security controls: SP 800-53, Center for Internet Security (CIS), ISO 27002, FAIR, and NISTIR 7621, introduced in the following paragraphs.

SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, provides an invaluable and extraordinarily detailed discussion of controls and should be consulted in the development of any risk treatment plan. This 450-page document provides plenty of guidance on the overall development of a treatment plan and includes a 233-page catalog of security controls (also available online) and a 55-page catalog of privacy controls. The security control catalog is organized according to the degree of impact each control addresses and includes 115 low-impact controls, 159 moderate-impact controls, and 170 high-impact controls. The controls are organized into the following families:



Online Catalog of Security Controls https://nvd.nist.gov/800-53/

- **AC:** Access Control
- **AU:** Audit and Accountability
- **AT:** Awareness and Training
- **CM:** Configuration Management
- **CP:** Contingency Planning
- **IA:** Identification and Authentication
- **IR:** Incident Response
- **MA:** Maintenance
- **MP:** Media Protection
- **PS:** Personnel Security
- **PE:** Physical and Environmental Protection
- **PL:** Planning
- **PM:** Program Management
- **RA:** Risk Assessment

https://t.me/learningnets

- **CA:** Security Assessment and Authorization
- **SC:** System and Communications Protection
- **SI:** System and Information Integrity
- **SA:** System and Services Acquisition

For each control, the catalog provides a description of the control, supplemental guidance on implementation, a description of control enhancements, and references to other documents.

Also worthwhile is the CIS Critical Security Controls for Effective Cyber Defense, described in Section 1.7. Table 1.10 in Chapter 1 provides the current list that CIS considers most important: 20 controls that encompass the broad range of known threats and the state of the art in countering those threats. There is also a companion document, *A Measurement Companion to the CIS Critical Security Controls*, that describes in detail techniques for measuring the performance of a given sub-control, plus a set of three risk threshold values (lower, moderate, and higher).

ISO 27002, *Code of Practice for Information Security Controls*, is a 90-page document with a well-organized list of controls (refer to Table 1.4 in Chapter 1), together with guidance on the implementation of each control.

For purposes of risk assessment, it is useful to group security controls in a manner that reflects the risk assessment process. The FAIR (Factor Analysis of Information Risk) risk analysis document, which is described in Section 3.6, groups controls into four categories.

- **Avoidance controls:** These controls, which include the following, affect the frequency and/or likelihood of encountering threats:
  - Firewall filters
  - Physical barriers
  - The relocation of assets
  - The reduction of threat populations (for example, reducing the number of personnel who are given legitimate access to assets)
- **Deterrent controls:** These controls, which include the following, affect the likelihood of a threat acting in a manner that results in harm (probability of action):
  - Policies
  - Logging and monitoring

https://t.me/learningnets

- Enforcement practices
- Asset hardening (for example, many threat actors are opportunistic in nature and gravitate toward easier targets, rather than targets that are perceived to be difficult)
- Physical obstacles (for example, external lights on building, barbed-wire fencing)

- **Vulnerability controls:** These controls, which include the following, affect the probability that a threat's action will result in loss (vulnerability):
  - Authentication
  - Access privileges
  - Patching
  - Configuration settings
- **Responsive controls:** These controls, which include the following, affect the amount of loss that result from a threat's action (loss magnitude):
  - Backup and restore media and processes
  - Forensics capabilities
  - Incident response processes
  - Credit monitoring for persons whose private information has been compromised

The following useful checklist of controls is also provided in NISTIR 7621:

- Identity
  - Identify and control who has access to your business information
  - Conduct background checks
  - Require individual user accounts for each employee
  - Create policies and procedures for information security
- Protect
  - Limit employee access to data and information
  - Install surge protectors and uninterruptible power supplies (UPSs)
  - Patch your operating systems and applications

https://t.me/learningnets

- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

- Detect
  - Install and update antivirus, anti-spyware, and other anti-malware programs
  - Maintain and monitor logs
- Respond
  - Develop a plan for disasters and information security incidents (for example, incident response plan)
- Recover
  - Make full backups of important business data/information
  - Make incremental backups of important business data/information
  - Consider cyber insurance
  - Make improvements to processes/procedure /technologies

The FAIR and NISTIR 7621 lists of controls provided here give you with some idea of the scale of the work involved in implementing an effective suite of security controls. Parts II, "Managing the Cybersecurity Function," and III, "Security Assessment," of this book discuss security controls in detail.

3.5 Vulnerability Identification

Vulnerability identification is the process of identifying vulnerabilities that can be exploited by threats to cause harm to assets. A vulnerability is a weakness or a flaw in a system's security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited when a threat is manifested.

The following sections develop categories of vulnerabilities, discuss approaches to identifying and documenting vulnerabilities, and discuss the use of the National Vulnerability Database.

https://t.me/learningnets

Vulnerability Categories

Vulnerabilities occur in the following areas:

- **Technical vulnerabilities:** Flaws in the design, implementation, and/or configuration of software and/or hardware components, including application software, system software, communications software, computing equipment, communications equipment, and embedded devices.
- **Human-caused vulnerabilities:** Key person dependencies, gaps in awareness and training, gaps in discipline, and improper termination of access.
- **Physical and environmental vulnerabilities:** Insufficient physical access controls, poor siting of equipment, inadequate temperature/humidity controls, and inadequately conditioned electrical power.
- **Operational vulnerabilities:** Lack of change management, inadequate separation of duties, lack of control over software installation, lack of control over media handling and storage, lack of control over system communications, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, inadequate control over encryption keys, inadequate reporting, handling and/or resolution of security incidents, and inadequate monitoring and evaluation of the effectiveness of security controls.
- **Business continuity and compliance vulnerabilities:** Misplaced, missing, or inadequate processes for appropriate management of business risks; inadequate business continuity/contingency planning; and inadequate monitoring and evaluation for compliance with governing policies and regulations.

In many of the areas listed here, vulnerability identification depends critically on management initiative and follow-through. Techniques such as interviews, questionnaires, review of previous risk assessments and audit reports, and checklists all contribute to developing a good picture of the vulnerability landscape.

National Vulnerability Database and Common Vulnerability Scoring System

In the area of technical vulnerabilities, it is possible to be more precise and exhaustive. An outstanding resource is the NIST National Vulnerability Database (NVD) and the related Common Vulnerability Scoring System (CVSS) [FIRS15], described in NISTIR 7946, *CVSS Implementation Guidance*. The NVD is a comprehensive list of known technical vulnerabilities in systems, hardware, and software. The CVSS provides an open framework for communicating the characteristics of vulnerabilities. The CVSS defines a vulnerability as a bug, a flaw, a weakness, or an exposure of an application, a system device, or a service that could lead to a failure of confidentiality,

https://t.me/learningnets

integrity, or availability. The CVSS model attempts to ensure repeatable and accurate measurement while enabling users to view the underlying vulnerability characteristics used to generate numeric scores. The CVSS provides a common measurement system for industries, organizations, and governments requiring accurate and consistent vulnerability exploit and impact scores.



NIST National Vulnerability Database
https://nvd.nist.gov

It is worthwhile to gain an understanding of the CVSS in order to understand the wide range of vulnerabilities that affect systems. In addition, the systematic scheme for evaluating vulnerabilities in the CVSS is useful in guiding the development of a similar systematic approach to other vulnerabilities such as those related to organizational issues, policies and procedures, and physical infrastructure. CVSS is widely accepted and used. For example, the Payment Card Industry Data Security Standard (PCI DSS) standard recommends use of CVSS.

Figure 3.4 provides an example of one of the vulnerability entries in the NVD.

Current Description
An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.
Source: MITRE **Last Modified:** 02/01/2017 View Analysis Description

CVSS Severity (version 3.0):
CVSS v3 Base Score: 8.8 High
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 2.8

CVSS Version 3 Metrics:
Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Quick Info
CVE Dictionary Entry: CVE-2017-3823
Original release date: 02/01/2017
Last revised: 04/04/2017
Source: US-CERT/NIST

FIGURE 3.4 NVD Scoring Example

Each NVD entry includes the following:

- The unique Common Vulnerabilities and Exposure (CVE) dictionary identifier
- A description of the vulnerability

https://t.me/learningnets

- Links to websites and other references with information related to the vulnerability
- CVSS metrics

There are 14 CVSS metrics in three groups. Table 3.6 lists the individual metrics and shows the levels defined for each one. In each case, the levels are listed from highest to lowest security concern. In essence, the scoring is done as follows: For each identified vulnerability, the NVD provides a level for each metric in the base group, based on the characteristics of the vulnerability. For example, the attack vector metric indicates whether the attack can be launched remotely over a network or over the Internet, is launched only across the immediate network to which both the attack source and the target system are attached, must be done by a local login, or requires physical access to the machine. The more remote the attack, the more attack sources are possible, and therefore the more serious the vulnerability. This information is invaluable in enabling users to understand the characteristics of a vulnerability.

TABLE 3.6 CVSS Metrics

Base Metric Group		Temporal Metric Group	Environmental Metric Group
Exploitability	**Impact**		
Attack Vector ■ Network ■ Adjacent ■ Local ■ Physical **Attack Complexity** ■ Low ■ High **Privileges Required** ■ None ■ Low ■ High **User Interaction** ■ None ■ Required	**Confidentiality Impact** ■ High ■ Low ■ None **Integrity Impact** ■ High ■ Low ■ None **Availability Impact** ■ High ■ Low ■ None	**Exploit Code Maturity** ■ Not defined ■ High ■ Functional ■ Proof-of-concept ■ Unproven **Remediation Level** ■ Not defined ■ Workaround ■ Temporary fix ■ Official fix **Report Confidence** ■ Not defined ■ Confirmed ■ Reasonable ■ Unknown	**Confidentiality Requirement** ■ Not defined ■ High ■ Medium ■ Low **Integrity Requirement** ■ Not defined ■ High ■ Medium ■ Low **Availability Requirement** ■ Not defined ■ High ■ Medium ■ Low
Scope ■ Unchanged ■ Changed			

As Table 3.6 shows, each level of a metric has a descriptive name. In addition, the CVSS assigns a numeric value on a scale of 0.0 to 10.0, with 10.0 being the most

https://t.me/learningnets

severe security issue. The numeric scores for the metrics in the base metric group are put into an equation defined in the CVSS that produces an aggregate base security score ranging from 0.0 to 10.0 (see Figure 3.4).

The base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It consists of three sets of metrics:

- **Exploitability:** These metrics reflect the ease and technical means by which the vulnerability is exploited. The metrics are:
  - **Attack vector:** As mentioned, this metric is a measure of how remote an attacker can be from the vulnerable component.
  - **Attack complexity:** Conveys the level of difficulty required for an attacker to exploit a vulnerability once the target component is identified. The complexity is rated high if the attacker cannot accomplish the attack at will but must invest some measurable amount of effort in preparation or execution.
  - **Privileges required:** Measures the access an attacker requires to exploit a vulnerability. The values are none (no privileged access required), low (basic user privileges), and high (administrative-level privileges).
  - **User interaction:** Indicates whether a user other than the attacker must participate for a successful attack.
- **Impact:** These metrics indicate the degree of impact on the primary security objectives confidentiality, integrity, and availability. In each of these cases, the score reflects the worst outcome if more than one component is affected (scope = changed). For each of the three objectives, the values are high (total loss of confidentiality, integrity, or availability), low (some loss), and none.
- **Scope:** This metric is grouped within the base metric group although it is somewhat independent of the remainder of the group. It refers to the ability for a vulnerability in one software component to impact resources beyond its means, or privileges. An example is a vulnerability in a virtual machine that enables an attacker to delete files on the host operating system. An unchanged value of this metric means that the vulnerability can only affect resources managed by the same authority.

Generally, the base and temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors because they typically have better information about the characteristics of a vulnerability than do users. The environmental metrics, however, are specified by users because they are best able to assess the potential impact of a vulnerability within their own environments.

https://t.me/learningnets

The temporal metric group represents the characteristics of a vulnerability that change over time but not among user environments. It consists of three metrics. In each case, the value "not defined" indicates that this metric should be skipped in the scoring equation.

- **Exploit code maturity:** This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability. The levels reflect the degree to which the exploit is available and usable for exploiting the vulnerability.
- **Remediation level:** Measures the degree to which remediation is available.
- **Report confidence:** Measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details.

The environmental metric group captures the characteristics of a vulnerability that are associated with a user's IT environment. It enables the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user's organization, measured in terms of confidentiality, integrity, and availability.

3.6 Risk Assessment Approaches

This section begins with a discussion of the distinction between quantitative and qualitative risk assessment. This is followed by discussion of a simple approach to risk assessment. Finally, this section provides an overview of FAIR, which is referenced several times elsewhere in this chapter.

Quantitative Versus Qualitative Risk Assessment

Two factors of risk assessment can be treated either quantitatively or qualitatively: impact and likelihood. For impact, if it seems feasible to assign a specific monetary cost to each of the impact areas, then the overall impact can be expressed as a monetary cost. Otherwise, qualitative terms, such as low, moderate, and high, are used. Similarly, the likelihood of a security incident may be determined quantitatively or qualitatively. The quantitative version of likelihood is simply a probability value, and again the qualitative likelihood can be expressed in such categories as low, medium, and high.

Quantitative Risk Assessment

If all factors are expressed quantitatively, then it is possible to develop a formula such as the following:

$$\text{Level of risk} = (\text{Probability of adverse event}) \times (\text{Impact value})$$

https://t.me/learningnets

This is a measure of the cost of security breaches, expressed numerically. It can also be expressed as a residual risk level as follows:

$$\text{Residual risk level} = \frac{(\text{Probability of adverse event})}{(\text{Mitigation factor})} \times (\text{Impact value})$$

In this equation, the mitigation factor reflects the reduction in the probability of an adverse event due to the implementation of security controls. Thus, the residual risk level is equivalent to the expected cost of security breaches with the implementation of controls.

If the various factors can be quantified with a reasonable degree of confidence, then these equations should be used to guide decisions concerning how much to invest in security controls. Figure 3.5 illustrates this point: As new security controls are implemented, the residual probability of an adverse event declines and, correspondingly, the cost of security breaches declines. However, at the same time, the total cost of security controls increases as new controls are added. The upper curve represents the total security cost, consisting of the cost of security breaches plus the cost of security controls. The optimal cost point occurs at the lowest point of the total cost curve. This represents a level of risk that is tolerable and cannot be reduced further without the expenditure of costs that are disproportionate to the benefit gained.

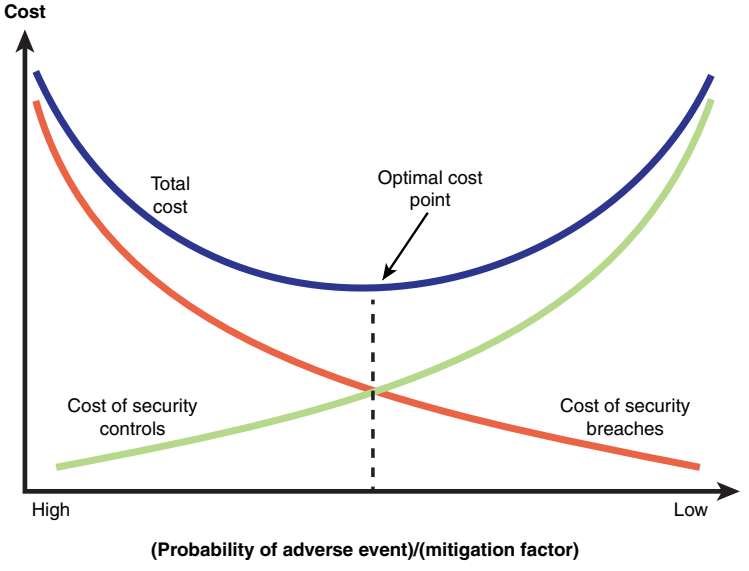


FIGURE 3.5 Cost Analysis for Risk Assessment

Qualitative Risk Assessment

It is not reasonable to suppose that all impact costs and likelihoods can with confidence be expressed quantitatively. Security breaches are rare, and organizations are

https://t.me/learningnets

reluctant to reveal them. Consequently, security incidence information is typically anecdotal or based on surveys and cannot be used to develop reliable or accurate probability or frequency values. At the same time, the total cost or potential loss due to a security breach is hard to quantify. The cost may depend on a variety of factors, such as length of downtime, amount and effect of adverse publicity, cost to recover, and other factors that are difficult to estimate.

However, it is possible, using reasonable judgment, to use qualitative risk assessment effectively. Qualitative assessment determines a relative risk rather than an absolute risk. This considerably simplifies the analysis, producing rough estimates of risk levels. Qualitative risk assessment is usually sufficient for identifying the most significant risks and allowing management to set priorities for security expenditures with a reasonable degree of confidence that all the significant risks have been mitigated. Table 3.7 compares quantitative and qualitative risk assessment.

TABLE 3.7 Comparison of Quantitative and Qualitative Risk Assessment

	Quantitative	Qualitative
Benefits	■ Risks are prioritized by financial impact; assets are prioritized by financial values. ■ Results facilitate management of risk by return on security investment. ■ Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage). ■ Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.	■ It enables visibility and understanding of risk ranking. ■ It is easier to reach consensus. ■ It is not necessary to quantify threat frequency. ■ It is not necessary to determine financial values of assets. ■ It is easier to involve people who are not experts on security or computers.
Drawbacks	■ Impact values assigned to risks are based on subjective opinions of participants. ■ The process to reach credible results and consensus is very time-consuming. ■ Calculations can be complex and time-consuming. ■ Results are presented in monetary terms only, and they may be difficult for nontechnical people to interpret. ■ The process requires expertise, so participants cannot be easily coached through it.	■ There is insufficient differentiation between important risks. ■ It is difficult to justify investing in control implementation because there is no basis for a cost/benefit analysis. ■ Results are dependent upon the quality of the risk management team that is created.

https://t.me/learningnets

Note in Table 3.7 that "impact values assigned to risks are based on subjective opinions of participants" is listed as a drawback of quantitative risk assessment. This is because it is not feasible to predict the cost of an impact within tight quantitative values. The official or group involved must make a subjective assessment of what the quantitative value will be for some future event. Disregarding this limitation may lead to a false impression of the accuracy of quantitative risk assessment. It is also true that subjective opinions are used to make a qualitative estimate of impact, but in this latter case, it is clear that subjective estimates are inherent in the process.

An organization needs some clearly defined categories of impact, threat, and vulnerability. For impact, FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines three security categories based on the potential impact on an organization should certain events occur that jeopardize the IT assets needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The categories are as follows:

- **Low:** Expected to have a limited adverse effect on organizational operations, organizational assets, or individuals, including the following:
  - Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
  - Result in minor damage to organizational assets
  - Result in minor financial loss
  - Result in minor harm to individuals
- **Moderate or medium:** Expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, including the following:
  - Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
  - Result in significant damage to organizational assets
  - Result in significant financial loss
  - Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
- **High:** Expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, including the following:
  - Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions

https://t.me/learningnets

- Result in major damage to organizational assets
- Result in major financial loss
- Result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides a number of examples of qualitative impact assessment. For example, say that a law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}.

Similarly, ranges of probability are assigned to qualitative likelihood categories. SP 800-100, *Information Security Handbook: A Guide for Managers*, suggests the following categories:

- **Low:** ≤0.1
- **Medium:** 0.1 to 0.5
- **High:** 0.5 to 1.0

Another possible categorization is based on an estimate of the number of times per year an event occurs:

- **Low:** <1 time per year
- **Medium:** 1 to 11 times per year
- **High:** >12 times per year

With these categories in mind, Figure 3.6 illustrates the use of matrices to determine risk. The vulnerability to a particular threat is a function of the capability, or strength, of the threat and the resistance strength of a system or an asset to that particular threat. Then, the likelihood of an adverse security event causing a particular threat is a function of the frequency, or likelihood, of the threat occurring and the vulnerability to that threat. Impact is determined as a function of asset class and the exposure to loss that a particular threat could cause. For example, assets can be classified in terms of the business impact of a loss.

https://t.me/learningnets

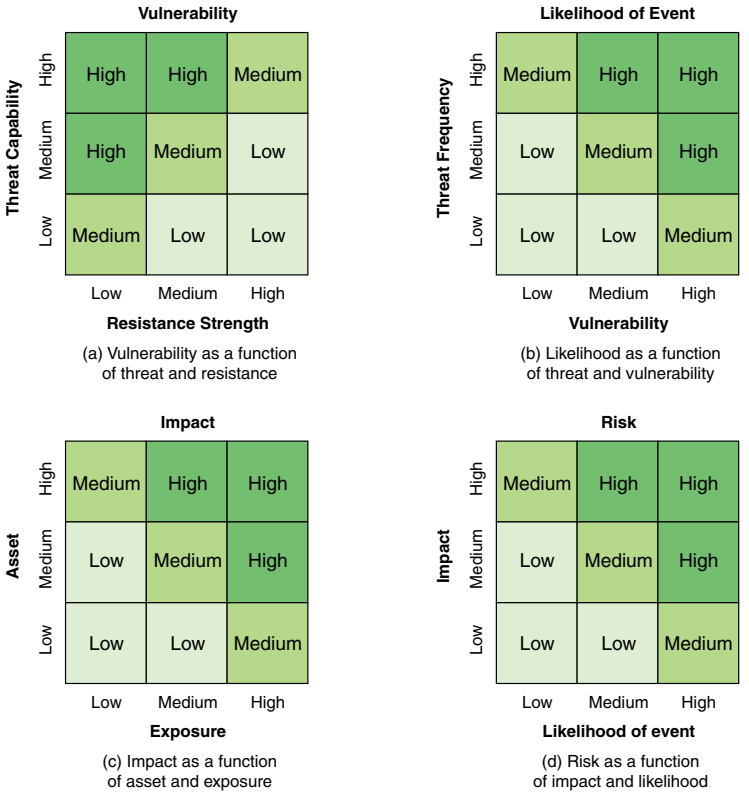


FIGURE 3.6 Qualitative Risk Determination

Review of Enterprise Security Risk Management [HIRT15] suggests the following classification examples:

- **Low business impact:** Public information, high-level information
- **Medium business impact:** Network designs, employee lists, purchase order information
- **High business impact:** Financial data, **personally identifiable information (PII),** Social Security numbers, medical record information

personally identifiable information (PII)
Information used to distinguish or trace an individual's identity, such as name, Social Security number, or biometric records, either alone or when combined with other information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, and so on.

Review of Enterprise Security Risk Management [HIRT15] also suggests the following exposure examples:

- **Low asset exposure:** Minor or no loss
- **Medium asset exposure:** Limited or moderate loss
- **High asset exposure:** Severe or complete loss

https://t.me/learningnets

Finally, risk is determined as a function of impact and the likelihood of an adverse event that causes the impact. Thus, these matrices, coupled with an informed estimate of low, medium, and high for the various factors, provide a reasonable means of assessing risk.

It should be kept in mind, however, that results of such a coarse-grained analysis must be subject to judgment. For example, in Figure 3.6d, a low-likelihood, high-impact breach and a high-likelihood, low-impact breach are both rated as medium risk. Which should be given priority for scarce security resources? On average, each type of breach may be expected to yield the same amount of annual loss. Is it more important to deal with the former breach—because although rare, if it does occur, it could be catastrophic for the organization—or deal with the latter type—which could produce a steady stream of losses. That is for management to decide.

Simple Risk Analysis Worksheet

A simple approach to risk assessment is to use a risk analysis worksheet, which is a table with one row for each potential threat/vulnerability pair [GADS06]. This worksheet, prepared by the risk assessment team, contains the following columns:

- **Security issue:** A brief statement of each security issue or area of concern. There should be one row for each threat/vulnerability pair (as well as compliance issues, described subsequently).
- **Likelihood:** Estimated likelihood for an occurrence of this threat/vulnerability pair. The estimate should be based on the team's judgment of the value of the affected assets and the magnitude of the exposure, using the matrices in Figures 3.6a and 3.6b.
- **Impact:** Estimated impact for this threat/vulnerability pair. The estimate should be based on the team's judgment of the affected assets value of the magnitude of the exposure, using the matrix in Figure 3.6c.
- **Risk level:** Risk level, based on the matrix in Figure 3.6d.
- **Recommended security controls:** Specific security control(s) that the team is recommending to address this particular issue.
- **Control priorities:** Relative priority of each recommended control.
- **Comments:** Any other information that is considered relevant to the security risk management decision-making process for this particular security issue.

Compliance issues can be documented on the same worksheet. Compliance requirements include those imposed by the organization's security policy, government regulations, and applicable accreditation standards. Compliance should be rated as follows:

0 = not implemented
1 = partially implemented

https://t.me/learningnets

2 = implemented but not yet documented
3 = implemented and documented

For compliance issues, the Likelihood and Impact fields are irrelevant. An issue with a compliance score of less than 3 should be included in the worksheet with a risk level of high.

MUSC Information Security Guidelines: Risk Management [GADS06] includes a number of examples of threat/vulnerability pairs, including the following:

- **Security issue:** An authorized employee uses the system in an unauthorized manner. **Threat:** Deliberate misuse of the system by an insider. **Vulnerability:** Inadequate training (the employee doesn't know better), or inadequate audit controls (the employee believes his misuse won't be detected), or lack of effective disciplinary process (employee believes there won't be any sanctions, even if his misuse is detected).
- **Security issue:** A serious, ongoing system compromise is not discovered until too late because nobody was checking up on the person who was assigned to review the system activity records that would have revealed the compromise. **Threat:** Deliberate unauthorized access. **Vulnerability:** Whatever vulnerability or vulnerabilities contributed to the original intrusion, compounded by inadequate monitoring and evaluation of the effectiveness of the system's audit controls.



Cybersecurity Book Resource Site https://app.box.com/v/ws-cybersecurity

The document resource site for this book provides three examples of simple risk analyses.

Factor Analysis of Information Risk

The Open Group
A global consortium with more than 500 member organizations that enables the achievement of business objectives through IT standards.

An important contribution to risk assessment is Factor Analysis of Information Risk (FAIR), first introduced in 2005. FAIR, which has been standardized by **The Open Group,** has received wide acceptance. Its relationship to International Organization for Standardization (ISO) risk standards are summarized as follows:

- ISO 27001 describes a general process for creating an information security management system (ISMS).
- In that context, ISO 27005 defines the approach to managing risk.
- FAIR provides a methodology for analyzing risk.

Thus, FAIR provides more specific guidance that can be used within the framework defined by ISO 27005.

https://t.me/learningnets

The Open Group has published four risk-related standards documents:

- **Risk Taxonomy:** This standard provides a rigorous set of definitions and taxonomy for information security risk as well as information regarding how to use the taxonomy.
- **Requirements for Risk Assessment Methodologies:** This technical guide identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements.
- **FAIR—ISO/IEC 27005 Cookbook:** This technical guide describes in detail how to apply the FAIR methodology to the ISO 27005 framework.
- **The Open Group Risk Analysis (O-RA) Technical Standard:** This document provides a set of standards for various aspects of information security risk analysis.

Open Group Security Standards http://www.opengroup.org/standards/security

Figure 3.7 illustrates the relationships between the three risk assessment tasks in ISO 27005 and the detailed definitions of those tasks in FAIR. FAIR provides a more detailed set of guidelines for all aspects of risk assessment. For example, FAIR provides definitions of the key terms that are less vague and more specifically tied to the risk analysis process than does ISO 27005.

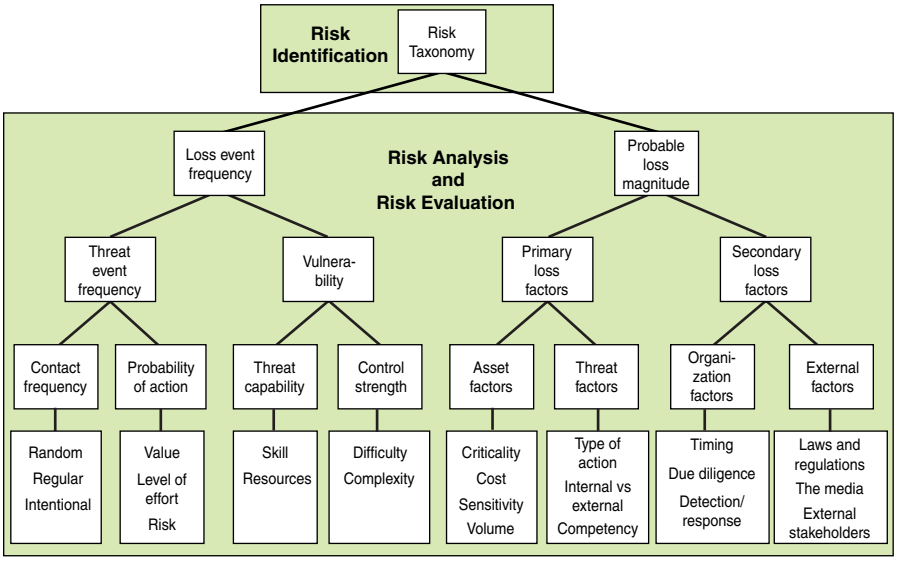


FIGURE 3.7 Risk Assessment Using FAIR

https://t.me/learningnets

The key FAIR definitions are as follows:

- **Asset:** Any data, device, or other component of the environment that supports information-related activities that can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.
- **Risk:** The probable frequency and probable magnitude of future loss.
- **Threat:** Anything that is capable of acting in a manner resulting in harm to an asset and/or organization—for example, acts of God (weather, geologic events, and so on), malicious actors, errors, and failures.
- **Vulnerability:** The probability that an asset will be unable to resist actions of a threat agent.

The FAIR methodology is based on a belief that subjective qualitative analysis is inadequate in most situations and that all risk, tangible and intangible, is measurable and quantifiable. The actual quantitative analysis results are delivered using calibrated, probabilistic estimates based on ranges of probabilities, accurate comparisons, and PERT calculations run through Monte Carlo simulations.

Both ISO 27005 and FAIR are referenced throughout this chapter.

3.7 Likelihood Assessment

In Figure 3.1, earlier in this chapter, the upper row of boxes relates to risk identification, which has been discussed in the preceding sections. The remainder of the figure relates to risk analysis, which consists of three tasks:

- Likelihood assessment
- Impact assessment
- Risk determination

This section examines likelihood assessment. Sections 3.8 and 3.9 discuss impact assessment and risk determination, respectively.

Likelihood assessment does not yield a numerical value subject to calculation using probability theory. Rather, it is the process of developing some sort of agreed-upon likelihood score that estimates the chance of a threat action. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the presence of vulnerabilities and the effectiveness of security controls already in place. This assessment is applied to each identified potential threat action.

https://t.me/learningnets

The essence of likelihood assessment for a given threat to a given asset is shown in the following steps:

Step 1. Determine the likelihood that a threat event will occur. That is, determine the likelihood that this threat will develop into an attack on the given asset.
Step 2. Determine the degree of vulnerability of the asset to the threat.
Step 3. Based on Step 1 and Step 2, determine the likelihood that a security incident will occur.

This analysis needs to be repeated for every threat to every asset.

ISO 27005 and other ISO documents provide limited guidance on how to perform this function. FAIR provides detailed guidance on how to systematically characterize event likelihood, referred to in the FAIR documents as *loss event frequency*. This guidance, although clear, is rather complex; this chapter provides an overview. As indicated in the left-hand portion of Figure 3.7, FAIR adopts a top-down approach to determining loss event frequency. At the top level, it may be possible, based on historical data, to develop an estimate of loss event frequency, simply on the basis of how frequently a loss event has occurred in the past. It is not necessary, and indeed not possible, to derive an exact frequency or probability. For one thing, a security event in the past may remain undetected at the time of the risk assessment. In addition, the past cannot be considered an exact predictor of the future. The examples in the FAIR documents use five levels (very low, low, moderate, high, very high) with an order of magnitude change between levels, as shown in Table 3.8.

TABLE 3.8 FAIR Risk Assessment Levels

Level	Loss Magnitude	Event Frequency	Threat Capability	Resistance Strength	Secondary Loss Probability
Very high (VH)	>1,000X	>100 times per year	Top 2% when compared against the overall threat population	Protects against all but the top 2% of an average threat population	90% to 100%
High (H)	100X to 1,000X	Between 10 and 100 times per year	Top 16% when compared against the overall threat population	Protects against all but the top 16% of an average threat population	70% to 90%

https://t.me/learningnets

Level	Loss Magnitude	Event Frequency	Threat Capability	Resistance Strength	Secondary Loss Probability
Moderate (M)	10X to 100X	Between 1 and 10 times per year	Average skill and resources (between bottom 16% and top 16%)	Protects against the average threat agent	30% to 70%
Low (L)	X to 10X	Between 0.1 and 1 times per year	Bottom 16% when compared against the overall threat population	Only protects against bottom 16% of an average threat population	10% to 30%
Very low (VL))	<X	<0.1 times per year (less than once every 10 years)	Bottom 2% when compared against the overall threat population	Only protects against bottom 2% of an average threat population	0% to 10%

X = monetary value assigned by organization

If the organization's management or security analysts do not have confidence that a good loss event frequency can be directly estimated, then the process is broken down into two tasks: estimating threat event frequency and estimating vulnerability.

Estimating Threat Event Frequency

The assessment of threat event frequency involves two aspects: determining the frequency with which a threat agent will come in contact with an asset and the probability that, once in contact, the threat agent will act against the asset.

Contact can be physical or logical. Physical access, for example, is possible for employees, contract workers such as cleaning and maintenance crews, and outside actors, such as clients, customers, salespeople, and inspectors. Logical access is via a network. Contact can be unplanned, or random, or it can be regular, such as with a cleaning crew, or it can be intentional, as when a hacker tries to gain logical access. The task for a security analyst is to come up with a reasonable estimate, such as using five levels (refer to Table 3.8) of frequency.

https://t.me/learningnets

The next task is to determine the probability or likelihood that the threat agent will take action, given that contact has been made. This, of course, depends on the nature of the threat and the type of action available to the threat agent. But in general, the factors that an analyst needs to consider are the perceived value to the threat agent in performing the action, the level of effort required to perform the act, and the risk of discovery and/or punishment if the action is detected.

Based on estimates of contact frequency and probability of action, the analyst should be able to make a reasonable estimate of the threat event frequency.

Estimating Vulnerability

As with the estimation of threat event frequency, the estimation of vulnerability involves assigning relative values to two dimensions. In the case of vulnerability, the two dimensions are the threat capability and the control strength. FAIR defines threat capability as the capability of the threat community to act against an asset using a specific threat. This needs to be expressed relative to some baseline, and the technique used in FAIR is to define five levels of threat capability that describe the strength of a specific threat relative to the overall threat population (refer to Table 3.8).

Estimating vulnerability involves looking at two factors:

- **Skill:** The knowledge and experience of the threat agent are critical factors in the severity of the threat action. Skill is reflected in the manner in which a threat agent is able to act, such as performing social engineering or bypassing logon or other access barriers. In the case of malware, the skill applied to constructing and propagating the malware determine the severity of the threat.
- **Resources:** The other important factor is the resources, such as the time, financial resources, and materials that a threat agent can bring to bear.

Thus, for a given threat to a given asset, the task of an analyst is to generate a reasonable estimate using the five threat capability levels shown in Table 3.8. For software-based threats, the CVSS discussed in Section 3.5 is a useful resource.

The other dimension of vulnerability is control strength, also referred to in the FAIR documents as *resistance strength*; it is also called *difficulty* by FAIR practitioners. This dimension relates to the asset's ability to resist compromise. The FAIR approach is to define five levels of resistance strength, based on the percentage of a threat population that an asset can successfully thwart, as shown in Table 3.8. The purpose of the controls is to increase the difficulty and complexity of causing a successful threat event. The more difficult that task is, the greater the capability the threat agent must have to overcome the controls currently in place.

https://t.me/learningnets

For a given threat to a given asset, once an analyst has developed estimates of threat capability and resistance strength, these two dimensions can be combined to produce a measure of vulnerability. This is done using the matrix shown in Figure 3.8a. (Compare this figure to Figure 3.6a.) As shown, the higher the resistance strength, the lower the vulnerability, and the higher the threat capability, the higher the vulnerability. The vulnerability values shown in the matrix are based on the experience of those involved in developing the FAIR model. For example, a high-threat capability applied to an asset with a low-resistance strength for that threat is rated as a very high vulnerability.

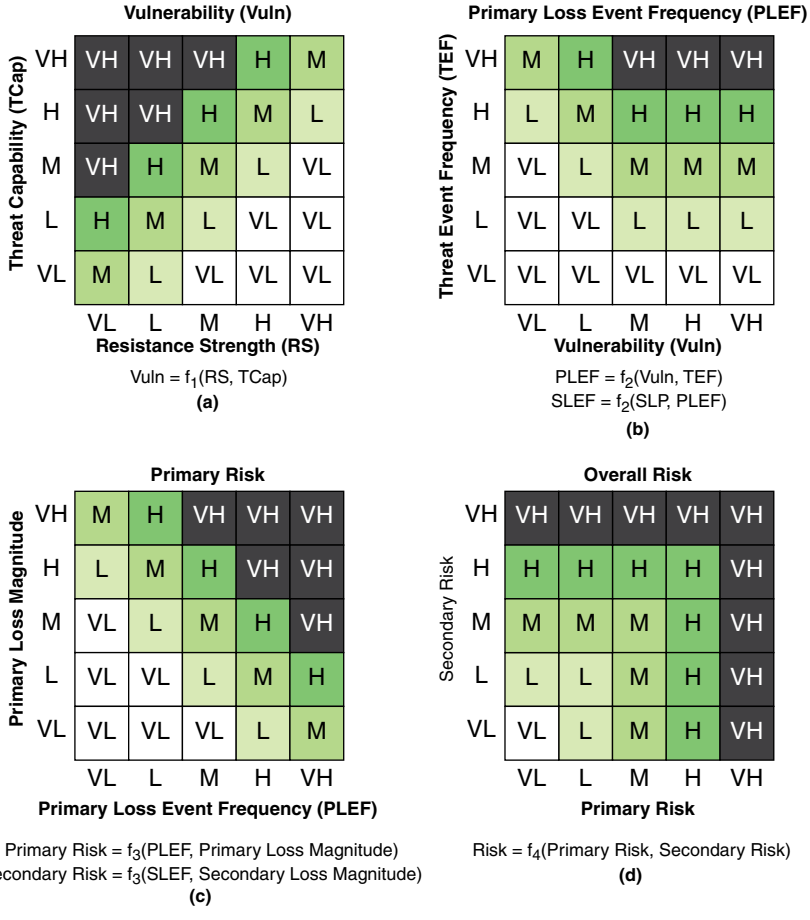


FIGURE 3.8 Sample FAIR Risk Assessment Matrices

It is worth making a distinction here between an estimated parameter and a derived parameter. Threat capability and resistance strength are parameters whose values are estimated by an analyst, which involves analytic effort. Once these two parameters are

https://t.me/learningnets

estimated, the analyst simply plugs them into the matrix to derive the desired vulnerability rating. The matrix defines a qualitative function, f_1, that is expressed as:

Vulnerability = f_1 (Resistance strength, Threat capability)

Loss Event Frequency

The likelihood of a loss, referred to as *loss event frequency* in the FAIR documents, is derived from the threat event frequency and vulnerability by using the matrix shown in Figure 3.8b. Again, the loss event frequency entries in the 5 × 5 matrix are based on judgments made by the FAIR designers. For example, if the threat event frequency is very high and the vulnerability is in the range of medium to very high, then the likelihood of a loss event is rated as very high. Note that the loss event frequency is limited by the threat event frequency; that is, the loss event frequency is never higher than the threat event frequency, no matter what the degree of vulnerability.

This matrix defines a function f_2:

Primary loss event frequency = f_2 (Vulnerability, Threat event frequency)

This derived quantity is also referred to as the *primary loss event frequency*, to contrast it with the secondary loss event frequency discussed subsequently.

SP 800-30 defines an approach to determining loss event frequency that is less complex than the FAIR approach. Table 3.9, adapted from SP 800-30, summarizes this approach. The table allows the use of either qualitative values or what the standard refers to as *semi-quantitative* values. This table is used both for adversarial and non-adversarial threats. The likelihood of a threat event combined with the likelihood that the threat event results in adverse impact are used as inputs to the matrix in Figure 3.8b to determine the likelihood of an adverse impact.

TABLE 3.9 Likelihood Assessment Scales

Qualitative Value	Semi-Quantitative Values	Likelihood of Threat Event Initiation (Adversarial)	Likelihood of Threat Event Occurrence (non-adversarial)	Likelihood of Threat Event Resulting in Adverse Impact
Very high	96–100	Adversary is almost certain to initiate the threat event.	Error, accident, or act of nature is almost certain to occur or occurs more than 100 times a year.	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.

https://t.me/learningnets

Qualitative Value	Semi-Quantitative Values	Likelihood of Threat Event Initiation (Adversarial)	Likelihood of Threat Event Occurrence (non-adversarial)	Likelihood of Threat Event Resulting in Adverse Impact
High	80–95	Adversary is highly likely to initiate the threat event.	Error, accident, or act of nature is highly likely to occur or occurs between 10 and100 times a year.	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21–79	Adversary is somewhat likely to initiate the threat event.	Error, accident, or act of nature is somewhat likely to occur or occurs between 1 and10 times a year.	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5–20	Adversary is unlikely to initiate the threat event.	Error, accident, or act of nature is unlikely to occur or occurs less than once a year but more than once every 10 years.	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very low	0–4	Adversary is highly unlikely to initiate the threat event.	Error, accident, or act of nature is highly unlikely to occur or occurs less than once every 10 years.	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

3.8 Impact Assessment

Impact assessment is the process of developing some sort of agreed-upon impact score or cost value that estimates the magnitude or the adverse consequence of a successful threat action.

The essence of impact assessment is that, for a given threat to a given asset, you determine the impact (cost or relative magnitude of impact) on the asset if the threat were to become an actual security incident. This analysis needs to be repeated for every threat to every asset.

ISO 27005 and other ISO documents provide limited guidance on how to perform this function. The FAIR documents note that this is one of the most difficult aspects of risk

https://t.me/learningnets

assessment. FAIR provides detailed guidance on how to systematically characterize impact. This guidance, although clear, is rather complex, so this section provides an overview.

FAIR impact analysis depends on two categories of loss, as shown Figure 3.7 and Table 3.10.

TABLE 3.10 FAIR Loss Categories

Loss Category	Loss Factors	Forms of Loss
Primary loss	■ **Asset:** Includes the value/liability characteristics of an asset and the volume of assets at risk ■ **Threat:** Includes type of action, whether internal or external, and threat competence.	■ **Productivity:** The reduction in an organization's ability to generate its primary **value proposition** (for example, income, goods, services). ■ **Response:** Associated with managing a loss event (for example, internal or external person-hours, logistical expenses). ■ **Replacement:** The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (for example, rebuilding a facility, purchasing a replacement laptop).
Secondary loss ■ Secondary loss event frequency ■ Secondary loss magnitude	■ **Organization:** Includes timing, due diligence, type of response, and detection capability. ■ **External:** Entities that can inflict a secondary form of harm upon the organization as a result of an event.	■ **Competitive advantage:** Losses associated with diminished competitive advantage; associated with assets that provide competitive differentiation between the organization and its competition. Examples include trade secrets and merger and acquisition plans. ■ **Fines/judgments:** Legal or regulatory actions levied against an organization. ■ **Reputation:** Associated with an external perception that an organization's value proposition is reduced or leadership is incompetent, criminal, or unethical.

value proposition

A statement that identifies clear, measurable, and demonstrable benefits to consumers when they buy a particular product or service. The value proposition should convince consumers that this product or service is better than others on the market.

The two loss categories are:

- **Primary loss:** Occurs directly as a result of the threat agent's action upon the asset. The owner of the affected assets is considered the primary stakeholder in an analysis. This event affects the primary stakeholder in terms of productivity loss, response costs, and so on.

https://t.me/learningnets

- **Secondary loss factors:** Occurs as a result of secondary stakeholders (for example, customers, stockholders, regulators) reacting negatively to the primary event. The reactions of the secondary stakeholders may, in turn, act as new threat agents against the organization's assets (such as reputation, legal fees, and so on), which, of course, affects the primary stakeholder.

Estimating the Primary Loss

For a given threat acting on a given asset, the FAIR impact (referred to as *loss* in the FAIR documents) assessment begins with determining the primary loss suffered as the result of the event. There are two aspects to this assessment:

- **Asset factors:** The value of the asset under threat.
- **Threat factors:** Threat factors that contribute to the loss.

The magnitude of the loss depends on a number of factors, such as how critical the asset is to the organization, the cost of replacement and/or recovery, and the sensitivity of information that might be disclosed or modified. The process of asset identification, discussed in Section 3.2, feeds into this evaluation.

The next step, for this asset and this threat, is to determine what threat action might apply to this asset. Possible actions include:

- **Access:** Simple unauthorized access
- **Misuse:** Unauthorized use of assets (for example, identity theft, setting up a pornographic distribution service on a compromised server)
- **Disclosure:** The threat agent illicitly disclosing sensitive information
- **Modification:** Unauthorized changes to an asset
- **Deny access:** Destruction or theft of a non-data asset

Other considerations are whether the threat agent is internal or external, which helps to indicate the motivation and intent of any threat event, and the ability of the threat agent to cause damage.

Once the asset and threat factors are understood, the analyst needs to determine the form of the loss, which includes productivity, response, and replacement (refer to Table 3.10). For each potential threat action, the analyst should estimate the probable loss magnitude for each form of loss. It is unrealistic to assign an exact monetary value to each loss. Rather, a hierarchy of levels can be used, with a monetary range for each level. The examples in the FAIR documents use five levels (very low, low, moderate, high, very high) with an order of magnitude change between levels

https://t.me/learningnets

(refer to Table 3.7). Once a loss magnitude is estimated for each form of loss, the maximum loss magnitude across all forms of loss is assigned as the primary loss magnitude for this asset and this threat.

Estimating the Secondary Loss

The estimation of secondary loss is more complex than the estimation of the primary loss. There are two components to this portion of the analysis:

- **Secondary loss magnitude:** Losses that are expected to materialize from dealing with secondary stakeholder reactions (for example, fines and judgments, loss of market share)
- **Secondary loss event frequency:** The percentage of time that a primary loss event is expected to result in a secondary loss as well

Estimating Secondary Loss Magnitude

The analysis of secondary loss magnitude proceeds in a manner similar to that for the primary loss. The analyst first determines the nature of the threat that applies in a given context and then determines the forms of loss and which form yields the greatest potential loss in this case.

Two sets of factors need to be considered in determining the nature of the threat:

- **Organizational factors:** Characteristics of the organization that determine the magnitude of the loss
- **External factors:** Entities that inflict a secondary form of harm upon the organization as a result of an event

A number of organizational factors need to be considered. For example, the timing of a security event in relationship to the organization's activities may determine how much loss is incurred. If a security event occurs just prior to a shareholders' meeting, the organization may not have time to react and resolve the problem before being held accountable by shareholders. The degree to which the organization has exercised due diligence, such as implementing a program in compliance with ISO 27001 and ISO 27002, can influence its degree of liability. The organization's ability to detect and rapidly respond contribute to its ability to contain secondary damage.

There are also external factors to consider. Laws and regulations can trigger penalties or sanctions for a security event. Public exposure of security failure can damage the organization's reputation. Customers or partners may be deterred from future business with the organization.

https://t.me/learningnets

Once the analyst has a grasp on the secondary loss possibilities, the next step is to determine the form of the loss, which includes competitive advantage, fines/judgments, and reputation (refer to Table 3.8). For each potential threat consequence, the analyst must estimate the probable loss magnitude for each form of loss, as is done for primary losses. Once a loss magnitude is estimated for each form of loss, the maximum loss magnitude across all forms of loss is assigned as the secondary loss magnitude for this asset and this threat.

Estimating Secondary Loss Event Frequency

To derive the secondary loss frequency, the analyst first needs to estimate the probability that a secondary stakeholder would be engaged, generating some form of secondary loss. The scale shown in the last column of Table 3.7 is used. This estimate is based on analyst judgment. To carry forward the analysis, it is necessary to convert this into a secondary loss frequency, using the matrix in Figure 3.7b. In functional form:

Secondary loss event frequency = f_2 (Secondary loss probability, Primary loss event frequency)

Note that this is the same matrix pattern used to evaluate the primary loss event frequency. Because a secondary loss is defined as one that may occur as a result of a primary loss, the secondary loss frequency must be less than or equal to the primary loss frequency, and this is reflected in the f_2 matrix.

Business Impact Reference Table

A useful tool for performing impact assessment is the Business Impact Reference Table (BIRT). The BIRT was developed by the ISF to enable all involved in the risk assessment process to have a common view of the risk elements. The BIRT provides consistent definitions to different types of impacts and severity levels. Typically, impact types include financial loss, reputation and image damage, stakeholder impact, and regulatory/statutory violations. Severity levels range from 1 (insignificant impact) through to 5 (catastrophic impact). The terminology in Table 3.7 indicates the type of common understanding of levels that is required.

Table 3.11 (A and B) is an example that shows part of the BIRT for a refining and marketing company specializing in premium-quality, lower-emission traffic fuels. The company has operations in 14 countries worldwide and employs some 5,000 people.

https://t.me/learningnets

TABLE 3.11A Example Business Impact Reference Table (part 1 of 2)

Impact Type	Unforeseen Impacts of Changes in Operations or Systems	Delayed Delivery to Customers or Clients	Loss of Customers or Clients	Loss of Confidence by Key Institutions and Partners	Damage to Corporate Image and Reputation
Measure	Extent of delay or halt in operations	Extent of delay	Percentage of customers lost	Extent of loss of confidence	Extent of negative publicity
Very high	Service delayed for 24 hours	Delivery delayed by 24 hours	>25%	Complete loss of confidence	Worldwide negative publicity
High	Service delayed for 12 hours	Delivery delayed by 12 hours	11% to 25%	Serious loss of confidence	Continentwide negative publicity
Moderate	Service delayed for 4 hours	Delivery delayed by 4 hours	6% to 10%	Significant loss of confidence	Nation-wide negative publicity
Low	Service delayed for 1 hours	Delivery delayed by 1 hours	1% to 5%	Moderate loss of confidence	Local negative publicity
Very low	Service delayed for 0.5 hours	Delivery delayed by 0.5 hours	<1%	Minor loss of confidence	Minor negative publicity

TABLE 3.11B Example Business Impact Reference Table (part 2 of 2)

Impact Type	Loss of Retail Customers	Loss of b-to-b Customers	Reduction in Staff Morale/ Productivity	Injury or Death
Measure	**Loss of Customers**	**Loss of Customers**	**Extent of Loss of Morale/ Productivity**	**Number of Incidents**
Very HIGH	>20%	>20%	Complete loss	Multiple loss of life
High	11% to 20%	11% to 20%	Serious loss	Loss of life
Moderate	6% to 10%	6% to 10%	Significant loss	Serious harm
Low	1% to 5%	1% to 5%	Moderate loss	Moderate harm
Very low	<1%	<1%	Minor loss	Minor harm

https://t.me/learningnets

3.9 Risk Determination

Once the loss magnitude is estimated and the loss event frequency derived, it is a straightforward process to derive an estimate of risk. This is done separately for primary and secondary losses, and then the two are combined.

The primary risk determination is illustrated in Figure 3.8c and is expressed as:

$$\text{Primary risk} = f_3 (\text{Primary loss event frequency, Primary loss magnitude})$$

The individual matrix values are a matter of judgment, which may differ from one organization to another. The matrix f_3 takes a relatively conservative view. Thus, if the loss magnitude is rated as very high, then the risk is assigned a value of very high even if the loss event frequency is only moderate. Similarly, even if the loss magnitude is rated as moderate, if the loss event frequency is rated as very high, the risk is assigned a value of very high.

The same f_3 calculation is applied to secondary loss to determine the secondary risk. The two risks are then combined to determine an overall risk using the matrix in Figure 3.8d, which is expressed as:

$$\text{Overall risk} = f_4 (\text{Primary risk, Secondary risk})$$

Again, the individual matrix values are a matter of judgment. For example, a conservative view might be that if both primary and secondary risk are at the same level, the overall risk should be raised to the next level. In that case, if both risks are rated high, the overall risk is rated very high. A less conservative strategy is indicated in function f_4.

3.10 Risk Evaluation

Once a risk analysis is done, senior security management and executives can determine whether to accept a particular risk and if not determine the priority in assigning resources to mitigate the risk. This process, known as risk evaluation, involves comparing the results of risk analysis with risk evaluation criteria.

The advice provided for risk evaluation, both by ISO 27005 and the FAIR documents, is general as the criteria developed vary significantly from one organization to another. ISO does make a distinction between risk evaluation criteria and risk acceptance criteria. Evaluation criteria focus on the importance of various business assets and the impact that can be caused to the organization by various security events. The goal is to be able to specify priorities for risk treatment. Risk acceptance criteria relate to how much risk the organization can tolerate and provide guidance on how much budget can be allocated for risk treatment.

https://t.me/learningnets

SP 800-100 provides some general guidance for evaluating risk and prioritizing action based on a three-level model:

- **High:** If an observation or a finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- **Moderate:** If an observation is rated as moderate risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
- **Low:** If an observation is described as low risk, the system's authorizing official must either determine whether corrective actions are still required or decide to accept the risk.

3.11 Risk Treatment

Once the risk assessment process is complete, management should have a list of all the threats posed to all assets, with an estimate of the magnitude of each risk. In addition, a risk evaluation provides input in terms of the priority and urgency with which each threat should be addressed. The response to the set of identified risks is referred to as *risk treatment* (or *risk response*), as shown in Figure 3.9.

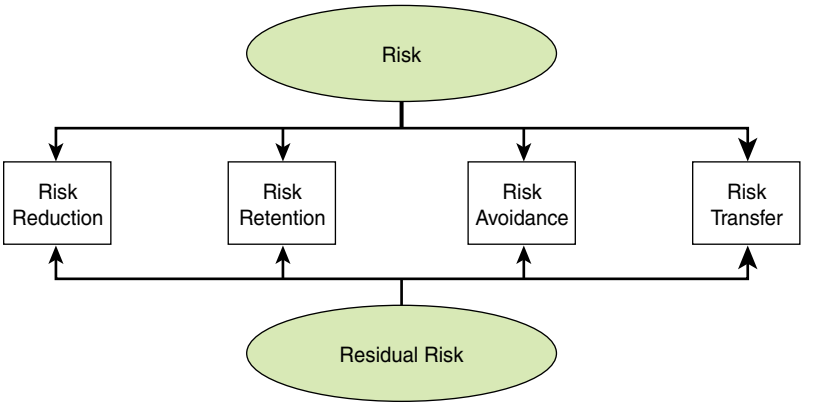


FIGURE 3.9 Risk Treatment

ISO 27005 lists these options for treating risk:

- **Risk reduction or mitigation:** Actions taken to lessen the probability and/or negative consequences associated with a risk
- **Risk retention:** Acceptance of the cost from a risk

https://t.me/learningnets

- **Risk avoidance:** Decision not to become involved in, or action to withdraw from, a risk situation
- **Risk transfer or sharing:** Sharing with another party the burden of loss from a risk

There is a many-to-many relationship between risks and treatments. A single treatment may affect multiple risks, and multiple treatments may be applied to a single risk. Further, the four options are not mutually exclusive. Multiple strategies may be adopted as part of a risk treatment plan.

Any risk treatment plan can reduce but not eliminate risk. What remains is referred to as *residual risk*. On the basis of the plan, the organization should update the risk assessment and determine whether the residual risk is acceptable or whether the plan needs to be updated.

Risk Reduction

Risk reduction is achieved by implementing security controls. Security controls can result in the following:

- Removing the threat source
- Changing the likelihood that the threat can exploit a vulnerability
- Changing the consequences of a security event

Part II of this book is devoted to risk reduction techniques.

Risk Retention

Risk retention, also called *risk acceptance*, is a conscious management decision to pursue an activity despite the risk presented or to refrain from adding to the existing controls, if any, in place to protect an asset from a given threat. This form of treatment, which is in fact non-treatment, is acceptable if the defined risk magnitude is within the risk tolerance level of the organization. In particular cases, the organization may accept risk that is greater than usually acceptable if a compelling business interest presents itself. In any case, the risk needs to be monitored and response plans that are acceptable to the stakeholders must be in place.

Risk Avoidance

If the risk in a certain situation is considered too high and the costs of mitigating the risk down to an acceptable level exceed the benefits, the organization may choose to

https://t.me/learningnets

avoid the circumstance leading to the risk exposure. This could mean, for example, forgoing a business opportunity, relocating to avoid an environmental threat or legal liability, or banning the use of certain hardware or software.

Risk Transfer

Sharing or transferring risk is accomplished by allocating all or some of the risk mitigation responsibility or risk consequence to some other organization. This can take the form of obtaining insurance or subcontracting or partnering with another entity.

3.12 Risk Assessment Best Practices

The SGP breaks down the best practices in the information risk assessment category into 2 areas and 12 topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Information risk assessment framework:** The objective of this area is to conduct regular information risk assessments for target environments (for example, critical business environments, processes, and applications, including supporting systems/networks) in a rigorous, consistent manner, using a systematic, structured methodology.
  - **Information risk assessment—management approach:** Summarizes tasks to enable individuals who are responsible for target environments to identify key information risks, evaluate them, and determine the treatment required to keep those risks within acceptable limits.
  - **Information risk assessment—methodology:** Summarizes a systematic and structured methodology to make information risk assessments effective, easy to conduct, and consistent throughout the organization and to produce a clear picture of key information risks. The document recommends the use of ISO 27005 and NIST SP 800-30 for detailed guidance.
  - **Information risk assessment—supporting material:** Describes supporting material needed to ensure that each phase of a risk assessment is performed correctly, assessments provide practical results, and effective decisions about risk can be made. The document recommends using BIRT and developing a set of security controls based on ISO 27002 and the NIST Cybersecurity Framework.
- **Information risk assessment process:** The objective of this area is to adopt an information risk assessment methodology that includes important activities covering scoping, business impact assessment, threat profiling, vulnerability assessment, risk evaluation, and risk treatment.

https://t.me/learningnets

- **Risk assessment scope:** Describes elements that define the scope of the risk assessment, including services, assets, and other factors influencing impact ratings (for example, economic, social, technological, legal, and environmental).
- **Business impact assessment:** Provides checklists for determining how a compromise of the confidentiality, integrity. and availability of information could have a business impact. This topic provides general guidance on using BIRT, determining best-guess and worst-case impacts, and determining financial, operational, and other impacts.
- **Business impact assessment—confidentiality requirements:** Repeats the checklists from the general business impact assessment.
- **Business impact assessment—integrity requirements:** Repeats the checklists from the general business impact assessment.
- **Business impact assessment—availability requirements:** Repeats the checklists from the general business impact assessment and also discusses metrics specific to availability.
- **Threat profiling:** Includes identifying, characterizing, and prioritizing threats. It also includes determining related threat events. The focus of this topic is characterization of the likelihood and strength of each identified threat.
- **Vulnerability assessment:** Lists considerations for evaluating the degree to which the assets in scope are vulnerable to each threat event.
- **Risk evaluation:** Discusses steps for performing risk evaluation, based on ISO 7005 and SP 800-30.
- **Risk treatment**: Discusses the process of creating a risk treatment plan.

3.13 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

asset
asset identification
Business Impact Reference Table (BIRT)
blockchain
consequence
consequences identification
container virtualization
control identification
impact
impact level
impact value

https://t.me/learningnets

kill chain
level of risk
likelihood
likelihood assessment
loss event frequency
network function virtualization (NFV)
personally identifiable information (PII)
primary loss
qualitative risk assessment
quantitative risk assessment
residual risk
risk
risk aggregation
risk analysis
risk assessment
risk criteria
risk determination
risk evaluation
risk identification
risk management
risk mitigation
risk of exposure (RoE)
risk reduction
risk retention
risk transfer
risk treatment
secondary loss
security control
security event
security incident
security operations center (SOC)
software-defined networking (SDN)
The Open Group
threat
threat event frequency
threat identification
value proposition
virtual machine
vulnerability
vulnerability identification

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Why is risk assessment needed in an organization?
2. Explain the term *residual risk* and provide an example.
3. Differentiate between a threat and a vulnerability.
4. What are the four factors that determine risk, and how are they related to each other?
5. Differentiate between qualitative and quantitative risk assessment.
6. Explain key ingredients of a risk analysis worksheet.
7. Explain the six stages of the information security risk management process.
8. Name the four risk-related standard documents that are published by The Open Group.
9. How does FAIR define key terms related to risk assessment? Is it more or less specific than ISO 27005 in its definitions pertaining to risk analysis?

https://t.me/learningnets

10. What are the different types of assets from a risk assessment point of view?
11. Explain the STRIDE threat model and provide an example.
12. List some common cybersecurity threat forms.
13. What are the three key themes of the *Threat Horizon 2019* report?
14. How does the FAIR risk analysis document group severity controls?
15. According to ISO 27005, what are viable options for any system that treats risk?
16. What elements comprise the scope of rick assessment?

3.14 References

ASHO17: Ashok, I., "Hackers Spied and Stole from Millions by Exploiting Word Flaw as Microsoft Probed Bug for Months." Inte*rnational Business Times*, April 27, 2017.

ENGE14: Engel, G., "Deconstructing the Cyber Kill Chain." *DarkReading*, November 18, 2014. http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542.

ENIS18: European Union Agency for Network and Information Security. *ENISA Threat Landscape Report 2017.* January 2018 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

FIRS15: First.org, Inc., *Common Vulnerability Scoring System v3.0: Specification Document*. 2015.

GADS06: Gadsden, R., *MUSC Information Security Guidelines: Risk Management*. Medical University of South Carolina, 2006. https://mainweb-v.musc.edu/security/guidelines/.

HERN06: Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Uncover Security Design Flaws Using the STRIDE Approach." *MSDN Magazine*, November 2006.

HIRT15: Hirt, R., *Review of Enterprise Security Risk Management*. 2015. https://www.slideshare.net/randhirt/review-of-enterprise-security-risk-management.

KEIZ17: Keizer, G., "Experts Contend Microsoft Canceled Feb. Updates to Patch NSA Exploits." *ComputerWorld*, April 18, 2017.

https://t.me/learningnets

MILL17: Millet, L., Fischhoff, B., & Weinberger, P. (Eds.), *Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions.* National Academies of Sciences, Engineering, and Medicine, 2017.

MYER13: Myers, L. "What is the cyber kill chain? Why it's not always the right approach to cyber attacks."*CSO*, dated November 7, 2017. https://www.cio.com/article/2381947/security0/the-practicality-of-the-cyber-kill-chain-approach-to-security.html.

RITC13: Ritchie, S., *Security Risk Management*. August 20, 2013. http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Security%20Risk%20Management.pdf.

RUBE14: Rubenking, N., "Trustwave Global Security Report Is Bursting with Valuable Data." *PCMag*, May 22, 2014.

https://t.me/learningnets

Chapter 4

Security Management

That Sir Henry should have been exposed to this is, I must confess, a reproach to my management of the case, but we had no means of foreseeing the terrible and paralyzing spectacle which the beast presented, nor could we predict the fog which enabled him to burst upon us at such short notice.

—*The Hound of the Baskervilles*, Sir Arthur Conan Doyle

Learning Objectives

After studying this chapter, you should be able to:

- List and explain the key security program areas that must be overseen by the security management function
- Explain the purpose and general content of a security plan
- Make a presentation on the topic of security-related capital planning
- Discuss the role and typical content of a security policy
- Discuss the role and typical content of an acceptable use policy
- Present an overview of security management best practices

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) describes security management as encompassing several key elements. An organization should provide a sufficiently senior manager, such as a chief information security officer (CISO), with the authority and adequate resources for organizationwide information security. The CISO, or a similar individual, is responsible for supervising security-related projects, promoting information security throughout the organization, managing risk, and developing a comprehensive, approved information security policy.

This chapter looks at various aspects of security management.

https://t.me/learningnets

4.1 The Security Management Function

Broadly speaking, the security management function entails establishing, implementing, and monitoring an information security program, under the direction of a senior responsible person.

Security management involves multiple levels of management. The different levels of management contribute to the overall security program with various types of expertise, authority, and resources. In general, executive managers (such as those at the headquarters level) best understand the organization as a whole and have more authority. On the other hand, frontline managers (at the IT facility and applications levels) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and the users. The levels of computer security program management should be complementary so that each can help the others be more effective.

Recall that Chapter 2, "Security Governance," defines two individual roles:

- **Chief information security officer (CISO):** The CISO has overall responsibility for the enterprise information security program. The CISO is the liaison between executive management and the information security program. The CISO should also communicate and coordinate closely with key business stakeholders to address information protection needs. The CISO is responsible for:
  - Establishing and maintaining an ISMS
  - Defining and managing an information security risk treatment plan
  - Monitoring and reviewing the ISMS
- **Information security manager (ISM):** The ISM has responsibility for the management of information security efforts. COBIT 5 lists the following as areas of responsibility:
  - Application information security
  - Infrastructure information security
  - Access management
  - Threat and incident management
  - Risk management
  - Awareness program
  - Metrics
  - Vendor assessments

https://t.me/learningnets

COBIT 5 makes a distinction between the CISO and the ISM, with the CISO being a C-level position with oversight of an ISM, who has operational management responsibilities. Some organizations combine the roles of CISO and ISM. For purposes of this chapter, we simply refer to this role as CISO.

NISTIR 7359, *Information Security Guide for Government Executives*, provides a useful summary of the tasks that comprise information security management Although addressed to government executives, NISTIR 7359 discusses the general functional areas of an information security or cybersecurity program that should be the responsibility of the CISO in any organization. The key security program areas include the following:

- **Security planning:** Security planning includes strategic security planning, which is defined in Chapter 2 as the alignment of information security management and operation with enterprise and IT strategic planning. But it also includes more detailed planning for the organization, coordination, and implementation of security. Key actors within the organization, such as department heads and project managers, need to be consulted and brought into the ongoing process of planning. Security planning is discussed in more detail in the following section.

capital planning

A decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of an organization's missions and business needs.

- **Capital planning:** Capital planning is designed to facilitate and control the expenditure of the organization's funds. Part of the planning process, and part of the CISO's responsibility, is to prioritize potential IT security investments for allocating available funding. Capital planning overlaps with security planning and is discussed subsequently in this section.
- **Awareness and training:** Awareness and training programs ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information resources entrusted to them. Chapter 5, "People Management," covers this topic.
- **Information security governance:** The CISO should advise C-level executives and the board concerning the development of effective security governance, which is covered in Chapter 2.
- **System development life cycle:** This is the overall process of developing, implementing, and retiring information systems. Chapter 8, "System Development," is devoted to this topic.
- **Security products and services acquisition:** Management supervision of the acquisition of security-related products and services includes considering the costs involved, the underlying security requirements, and the impact on the organizational mission, operations, strategic functions, personnel, and service-provider arrangements. Acquisition is discussed subsequently in this section.

https://t.me/learningnets

- **Risk management:** This topic is discussed in Chapters 2 and 3.
- **Configuration management:** The CISO should employ **configuration management** to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.
- **Incident response:** Incident response, which occurs after the detection of a security event, seeks to minimize the damage of the event and facilitate rapid recovery. The CISO should ensure that an adequate incident response system is in place and operating properly. Chapter 15, "Threat and Incident Management," covers this topic.
- **Contingency planning:** Information system contingency planning involves management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. Chapter 17, "Business Continuity," covers this topic.
- **Performance measures:** The CISO should ensure that an organizationwide performance measures are defined and used. Performance measures are a key feedback mechanism for an effective information security program. Chapter 18, "Security Monitoring and Improvement," covers this topic.

configuration management
The process of controlling modifications to a system's hardware, software, and documentation, which provides sufficient assurance that the system is protected against the introduction of improper modification before, during, and after system implementation.

Another useful source of guidance on the information management security function is the ISF SGP, which recommends that this function encompass the following:

- **Consistent organizationwide use of security:** The CISO (or equivalent) is responsible for developing, maintaining, and regularly reviewing an overall security strategy for the organization and the accompanying policy document.
- **Support function:** The CISO should:
  - Act as a clearinghouse for security advice, making experts available to business unit managers and project managers, as needed
  - Promote security awareness throughout the organization
  - Develop standard terms and agreements in contracts to ensure that suppliers and other external relationships meet the security standards of the organization
  - Evaluate the security implications of new business initiatives
  - Oversee the risk assessment process
  - Set standards for use of cryptographic algorithms and security protocols

https://t.me/learningnets

- **Monitor function:** The CISO should monitor trends and developments to be aware of how they may affect the organization's security strategy and implementation, including in the area of business trends, new technical developments, security solutions, standards, legislation, and regulation.
- **Projects function:** The CISO should be responsible for overseeing security-related projects.
- **External requirements function:** The CISO should manage the implications of laws, regulations, and contracts.

Security Planning

security plan
A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, indicates that the purpose of a system **security plan** is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan is basically documentation of the structured process of planning adequate, cost-effective security protection for a system.

SP 800-18 recommends that each information system in an organization have a separate plan document with the following elements:

- **Information system name/identifier:** A name or identifier uniquely assigned to each system. Assignment of a unique identifier supports the organization's ability to easily collect information and security metrics specific to the system as well as facilitate complete traceability to all requirements related to system implementation and performance. The identifier should remain the same throughout the life of the system and retained in audit logs related to system use.
- **Information system owner:** The person responsible for managing this asset.
- **Authorizing individual:** The senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.
- **Assignment of security responsibility:** The individual responsible for the security of the information system.
- **Security categorization:** Using the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, categories, the acceptable level of risk (low, moderate, or high) for confidentiality, integrity, and availability (for each distinct element of the system, if necessary).

https://t.me/learningnets

- **Information system operational status:** Status, such as operational, under development, or undergoing major modification.
- **Information system type:** Type, such as major application or support system.
- **Description/purpose:** A brief description (one to three paragraphs) of the function and purpose of the system.
- **System environment:** A general description of the technical system, including the primary hardware, software, and communications equipment.
- **System interconnections/information sharing:** Other systems/information assets that interact with this information system.
- **Related laws/regulations/policies:** Any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system.
- **Existing security controls:** Description of each control.
- **Planned security controls:** Description of each control plus implementation plan.
- **Information system security plan completion date:** The target date.
- **Information system security plan approval date:** The data plan approved date.

This sort of documentation enables the CISO to oversee all security projects throughout the organization. The CISO should also coordinate a process for developing and approving these plans. One good description of such a process is provided in *Federal Enterprise Architecture Security and Privacy Profile* [OMB10] and illustrated in Figure 4.1.

This process involves three steps, each of which has goals, objectives, implementing activities, and output products for formal inclusion in agency enterprise architecture and capital planning processes:

1. **Identify:** Encompasses the research and documentation activities necessary to identify security and privacy requirements in support of the mission objectives so that they can be incorporated into the enterprise architecture.
2. **Analyze:** Involves an analysis of organization security and privacy requirements and the existing or planned capabilities that support security and privacy.
3. **Select:** Involves an enterprise evaluation of the solutions proposed in the preceding phase and the selection of major investments.

https://t.me/learningnets

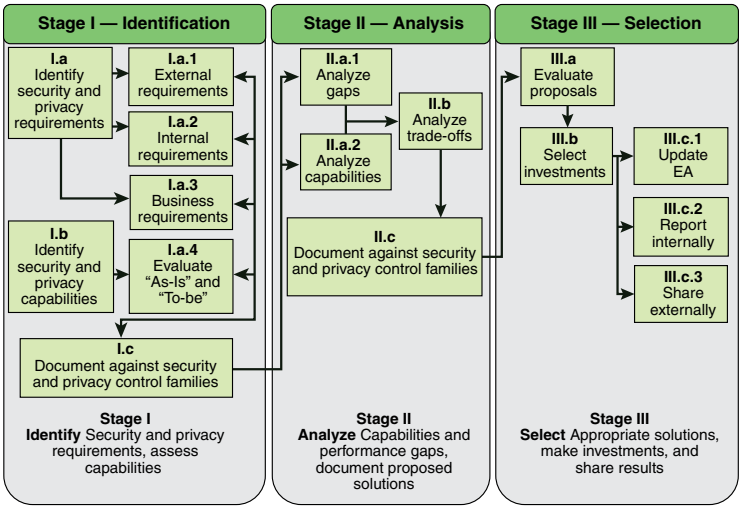


FIGURE 4.1 Example of a Security Planning Process

Step 1 refers to three types of requirements, defined as follows:

- **External requirements:** These are security requirements imposed from outside the organization, such as laws, regulations, and contractual commitments.
- **Internal requirements:** These are security requirements developed as part of the security policy, such as the acceptable degree of risk and confidentiality, integrity, availability, and privacy guidelines.
- **Business requirements:** This refers to requirements other than security requirements that are related to the overall business mission. Examples include finance, accounting, and audit requirements. In general, these requirements refer to the organization's need to discharge business responsibilities.

Capital Planning

Determining the benefit to an organization from IT security investments is a key element of IT security planning. Traditionally, capital planning has been applied to IT procurement overall and has been a separate function from security planning. As pointed out in NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, it is important to integrate capital planning methodology into the security planning process. An effective way of doing this—and one recommended by SP 800-65 is the Select/Control/Evaluate framework defined in the U.S. Government Accountability Office (GAO) publication *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* [GAO04], as shown in Figure 4.2.

https://t.me/learningnets

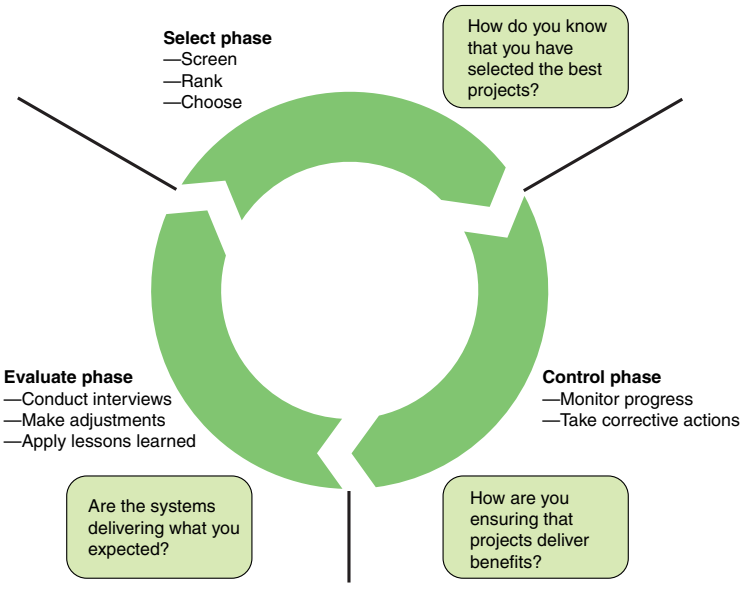


FIGURE 4.2 Capital Planning and Investment Lifecycle

The Select/Control/Evaluate framework defines a cyclical process consisting of three steps for deciding which projects to pursue or which investments to make:

1. **Select:** Identify and analyze each project's risks and returns before committing significant funds to any project. The organization then selects the IT projects that best support its mission needs. The organization repeats this process each time funds are allocated to projects.
2. **Control:** Ensure that as projects develops and investment expenditures continue, the project continues to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps must be quickly taken to address the deficiencies. If mission needs have changed, the organization needs to adjust its objectives for the project and appropriately modify expected project outcomes.
3. **Evaluate:** Compare actual results and expected results after a project was fully implemented. This is done for the following reasons:
    - To assess the project's impact on mission performance
    - To identify any necessary changes or modifications to the project
    - To revise the investment management process based on lessons learned

https://t.me/learningnets

Apply this process to every security-related investment in the organization. The costs typically incurred or contemplated are usually in three categories:

- Direct costs of providing IT security for the specific IT investment
- Costs for products, procedures, and personnel that have an incidental or integral component and/or a quantifiable benefit for the specific IT investment
- Allocated security control costs for networks that provide some or all necessary security controls for associated applications

Note that investment choices involve not only hardware and software but also procedures or processes within the organization. For example, risk assessment itself is a cost. How many employee-hours and at what levels should be devoted to this process? This includes effort to collect threat and vulnerability data from external sources, internal security incident review, and security-related reports from department heads, managers, and even individual employees. If the assessment is pursued to a great level of detail, the results may be well beyond the needs of the organization in making cost-effective decisions. Underinvestment may produce results that lack the breadth and depth necessary to reasonably protect assets. Similar considerations apply in other process-related costs, such as employee awareness efforts.

Table 4.1 describes the three categories in detail.

TABLE 4.1 Information Security Costs

Direct Costs	Products, Procedures, and Personnel	Allocated Security Control Costs
■ Risk assessment ■ Security planning and policy ■ Certification and accreditation ■ Specific security controls ■ Authentication or cryptographic applications ■ Education, awareness, and training ■ System reviews/ evaluations ■ Oversight or compliance inspections	■ Configuration or change management control ■ Personnel security ■ Physical security ■ Operations security ■ Privacy training ■ Program/system evaluations ■ System administrator functions ■ System upgrades with new features that obviate the need for other standalone security controls	■ Firewalls ■ Intrusion detection/ prevention systems ■ Forensic capabilities ■ Authentication capabilities ■ Additional add-on security considerations

https://t.me/learningnets

Direct Costs	Products, Procedures, and Personnel	Allocated Security Control Costs
■ Development or maintenance of security reports ■ Contingency planning and testing ■ Physical and environmental controls for hardware and software ■ Auditing and monitoring ■ Computer security investigations and forensics ■ Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations ■ Privacy impact assessments		

4.2 Security Policy

Recall from Chapter 2 that an information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. It is helpful to distinguish four types of documents before proceeding:

- **Information security strategic plan:** Relates to the long-term goals for maintaining security for assets.
- **Security plan:** Relates to security controls in place and planned to meet strategic security objectives.
- **Security policy:** Relates to the rules and practices that enforce security.
- **Acceptable use policy:** Relates to how users are allowed to use assets.

Table 4.2 provides a more detailed description. All these documents should be approved by a CISO or comparable executive. The CISO may task an individual or a team with document preparation. With these distinctions in mind, this section addresses security policy.

https://t.me/learningnets

TABLE 4.2 Security-Related Documents

Document Type	Description	Primary Audience
Information security strategic plan	A document used to communicate with the organization the organization's long-term goals with respect to information security, the actions needed to achieve those goals, and all the other critical elements developed during the planning exercise.	C-level executives
Security plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.	C-level executives, security managers, other managers
Security policy	A set of laws, rules, and practices that regulate how an organization manages and protects assets and the rules for distribution of sensitive information. It includes associated responsibilities and the information security principles to be followed by all relevant individuals.	All employees, especially those with some responsibility for an asset or assets
Acceptable use policy	A policy that defines for all parties the ranges of use that are approved for use of information, systems, and services within the organization.	All employees

The purpose of an information security policy is to ensure that all employees in an organization, especially those with responsibility of some sort for one or more assets, understand the security principles in use and their individual security-related responsibilities. Lack of clarity in information security policies can defeat the purpose of the security program and may result in significant losses. An information security policy is the means by which the organization provides management direction and support for information security across the organization. The security policy document defines what is expected from employees and possibly others who have roles in the organization, such as contractors, outside partners or vendors, and visitors.

Security Policy Categories

An organization may choose to use a single security policy document. For larger organizations, this may need to be a lengthy document. It is preferable to have a collection of policy documents so that employees and managers can consult only the relevant documents, as needed. Some of the security policies an organization may adopt include the following [INFO14]:

- **Access control policy:** How information is accessed
- **Contingency planning policy:** How availability of data is provided 24/7

https://t.me/learningnets

- **Data classification policy:** How data are classified
- **Change control policy:** How changes are made to directories or the file server
- **Wireless policy:** How wireless infrastructure devices need to be configured
- **Incident response policy:** How incidents are reported and investigated
- **Termination of access policy:** How employee access to organization assets is handled during termination
- **Backup policy:** How data is backed up
- **Virus policy:** How virus infections need to be dealt with
- **Retention policy:** How data can be stored
- **Physical access policy:** How access to the physical area is obtained
- **Security awareness policy:** How security awareness is carried out
- **Audit trail policy:** How audit trails are analyzed
- **Firewall policy:** How firewalls are named, configured, and so on
- **Network security policy:** How network systems are secured
- **Encryption policy:** How data are encrypted, the encryption method used, and so on
- **BYOD policy:** What devices an employee may use both on premises and off to access organization assets
- **Cloud computing policy:** Security aspects of using cloud computing resources and service

Ultimately, a CISO and a security manager are responsible for developing these policies. Typically, a security analyst or team of analysts are tasked with the actual formulation of policy documents, which are then approved by higher management.

Security Policy Document Content

Whether a single document or a set of documents, each security policy document should include the following sections:

- **Overview:** Background information on what issue the policy addresses
- **Purpose:** Why the policy was created
- **Scope:** What areas the policy covers
- **Targeted audience:** To whom the policy is applicable

https://t.me/learningnets

- **Policy:** A complete but concise description of the policy
- **Noncompliance:** Consequences for violating the policy
- **Definitions:** Technical terms used in the document
- **Version:** Version number to keep track of the changes made to the document

A good source of guidance for developing a policy document is the set of policy document templates provided by the SANS Institute. These have been made freely available as a public service. The complete set that is available is shown in Table 4.3.



SANS Institute Information Security Policy Templates https://www.sans.org/security-resources/policies/

TABLE 4.3 Security Policy Templates Provided by the SANS Institute

General	Network Security	Server Security	Application Security
Acceptable Encryption	Acquisition Assessment	Database Credentials	Web Application Security
Acceptable Use	Bluetooth Baseline Requirements	Technology Equipment Disposal	
Clean Desk	Remote Access	Information Logging Standard	
Data Breach Response	Remote Access Tools	Lab Security	
Disaster Recovery Plan	Router and Switch Security	Server Security	
Digital Signature Acceptance	Wireless Communication	Software Installation	
Email	Wireless Communication Standard	Workstation Security	
Ethics			
Pandemic Response Planning			
Password Construction Guidelines			
Password Protection			
Security Response Plan			
End User Encryption Key Protection			

As an example, the following sidebar shows one of the SANS Institute policy templates.

https://t.me/learningnets

SANS Institute Router and Switch Security Policy

1. **PURPOSE**
   This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of <Company Name>.
2. **SCOPE**
   All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. All routers and switches connected to Cisco production networks are affected.
3. **POLICY**
   Every router must meet the following configuration standards:
   1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
   2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
   3. The following services or features must be disabled: IP directed broadcasts; incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses; TCP small services; UDP small services; all source routing and switching; all web services running on router; cisco discovery protocol on Internet connected interfaces; Telnet, FTP, and HTTP services; Auto-configuration
   4. The following services should be disabled unless a business justification is provided: Cisco discovery protocol and other discovery protocols; dynamic trunking; scripting environments, such as the TCL shell
   5. The following services must be configured: password encryption; NTP configured to a corporate standard source
   6. All routing updates shall be done using secure routing updates.
   7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
   8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
   9. Access control lists for transiting the device are to be added as business needs arise.

https://t.me/learningnets

10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented for all forms of login whether remote or local:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including: IP access list accounting; device logging; incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped; router console and modem access must be restricted by additional security controls

4. POLICY COMPLIANCE

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 EXCEPTIONS

Any exception to the policy must be approved by the Infosec team in advance.

5.3 NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

https://t.me/learningnets

Management Guidelines for Security Policies

The SGP provides a useful set of guidelines for the creation, content, and use of security policy documents, which can be categorized as follows:

- **Responsibilities:** Identify the following:
  - Those responsible for ratifying policy document (for example, the board)
  - Responsibilities of all relevant individuals to comply with the policy
  - Individuals responsible for protecting specific assets
  - That all individuals must confirm the understanding of, acceptance of, and compliance with relevant policies and understand that disciplinary action will follow policy violation
- **Principles:** Specify the following:
  - All relevant assets to be identified and classified by value/importance
  - All assets protected with respect to CIA (confidentiality, integrity, and availability) and other security requirements
  - All laws, regulations, and standards complied with
- **Actions:** Specify the following:
  - That all individuals are made aware of the security policy and their responsibilities
  - That all assets are subject to risk assessment periodically and before a major change
  - That all breaches are reported in a systematic fashion
  - That auditing occurs periodically and as needed
  - That policy documents are reviewed regularly and as needed
- **Acceptable use:** Policies that include the following:
  - Documentation of what behaviors are required, acceptable, and prohibited with respect various assets
  - Responsibility for establishing, approving, and monitoring acceptable use policies

Monitoring the Policy

The CISO should designate an individual or a group responsible for monitoring the implementation of the security policy. The responsible entity should periodically

https://t.me/learningnets

review policies and make any changes needed to reflect changes in the organization's environment, asset suite, or business procedures. A violation-reporting mechanism is needed to encourage employees to report.

4.3 Acceptable Use Policy

An acceptable use policy (AUP) is a type of security policy targeted at all employees who have access to one or more organization assets. It defines what behaviors are acceptable and what behaviors are not acceptable. The policy should be clear and concise, and it should be a condition of employment for each employee to sign a form indicating that he or she has read and understood the policy and agrees to abide by its conditions.

The MessageLabs white paper *Acceptable Use Policies—Why, What, and How* [NAYL09] suggests the following process for developing an AUP:

1. **Conduct a risk assessment to identify areas of concern.** As part of the risk assessment process, identify the elements that need to go into an AUP.
2. **Create the policy.** The policy should be tailored to the specific risks identified, including liability costs. For example, the organization is exposed to liability if customer data is exposed. If the failure to protect the data is due to an employee's action or inaction, and if this behavior violates the AUP, and if this policy is clear and enforced, then this may mitigate the liability of the organization.
3. **Distribute the AUP.** This includes educating employees on why an AUP is necessary.
4. **Monitor compliance.** A procedure is needed to monitor and report on AUP compliance.
5. **Enforce the policy.** The AUP must be enforced consistently and fairly when it is breached.



SANS Institute AUP Template https://www.sans.org/security-resources/policies/general#acceptable-use-policy

An example of a template for an AUP is provided by the SANS Institute. It has a similar structure to the security policy template shown in Section 4.1. The heart of the document is the policy section, which covers the following areas:

- **General use and ownership:** Key points in this section include:
  - Employees must ensure that proprietary information is protected.
  - Access to sensitive information is allowed only to the extent authorized and necessary to fulfill duties.
  - Employees must exercise good judgment regarding the reasonableness of personal use.

https://t.me/learningnets

- **Security and proprietary information:** Key points in this section include:
  - Mobile devices must comply with the company's BYOD policies.
  - System- and user-level passwords must comply with the company's password policy.
  - Employees must use extreme caution when opening email attachments.
- **Unacceptable use—system and network activities:** Key points in this section include:
  - Unauthorized copying of copyrighted material
  - The prohibition against accessing data, a server, or an account for any purpose other than conducting company business, even with authorized access
  - Revealing your account password to others or allowing use of your account by others
  - Making statements about warranty unless it is a part of normal job duties
  - Circumventing user authentication or security of any host, network, or account
  - Providing information about, or lists of, company employees to outside parties
- **Unacceptable use—email and communication activities:** Key points in this section include:
  - Any form of harassment
  - Any form of spamming
  - Unauthorized use, or forging, of email header information
- **Unacceptable use—blogging and social media:** Key points in this section include:
  - Blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate company policy, is not detrimental to company's best interests, and does not interfere with an employee's regular work duties.
  - Any blogging that may harm or tarnish the image, reputation, and/or goodwill of company and/or any of its employees is prohibited.
  - Employees may not attribute personal statements, opinions, or beliefs to the company.

https://t.me/learningnets

4.4 Security Management Best Practices

The SGP breaks down the best practices in the security management category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Security policy management:** Discusses a specialist information security function, led by a sufficiently senior manager (e.g., a CISO), that is assigned adequate authority and resources to run information security-related projects; promote information security throughout the organization; and manage the implications of relevant laws, regulations and contracts.
  - **Information security policy:** Documents the governing body's direction on and commitment to information security and communicate it to all relevant individuals.
  - **Acceptable use policies:** Lists recommended actions for establishing AUPs, which define the organization's rules on how each individual (for example, an employee, a contractor) may use information and systems, including software, computer equipment, and connectivity.
- **Information security management:** Provides guidance for developing a comprehensive, approved information security policy (including supporting policies, standards, and procedures) and communicating it to all individuals who have access to the organization's information and systems.
  - **Information security function:** Ensures that good practice in information security is applied effectively and consistently throughout the organization.
  - **Information security projects:** Lists recommended actions for ensuring that all information security projects apply common project management practices, meet security requirements, and are aligned with the organization's business objectives.
  - **Legal and regulatory compliance:** Describes a process that should be established to identify and interpret the information security implications of relevant laws and regulations.

4.5 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

acceptable use policy (AUP)
capital planning
configuration management
information security strategic plan
security plan
security planning
security policy

https://t.me/learningnets

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

4.1 Define the security management function.

4.2 What are the two key individual roles in security management?

4.3 Explain key security program areas.

4.4 Describe the "select-control-evaluate" framework for capital planning.

4.5 Briefly explain the need of an effective information security policy. Also list different documents related to security.

4.6 Describe some common security policies of an organization.

4.7 What can be an effective structure of a security document?

4.8 What are the key aspects of security policy document?

4.9 What functions does information security management perform?

4.10 What do you understand by "acceptable use policy"?

4.6 References

INFO14: INFOSEC Institute, *Information Security Policies*. April 16, 2014. http://resources.infosecinstitute.com/information-security-policies/

GAO04: Government Accountability Office. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*. GAO-04-394G, March 2004.

NAYL09: Naylor, J., *Acceptable Use Policies—Why, What, and How*. MessageLabs White Paper, 2009. http://esafety.ccceducation.org/upload/file/Policy/AUP%20Legal%20advice.pdf

OMB10: Office of Management and Budget, NIST, and Federal Chief Information Officers Council, *Federal Enterprise Architecture Security and Privacy Profile.* 2010.

https://t.me/learningnets

https://t.me/learningnets

PART II

Managing the Cybersecurity Function

The basic idea is that the several components in any complex system will perform particular subfunctions that contribute to the overall function.

—*The Sciences of the Artificial,* Herbert Simon, 1969

CHAPTER 5: People Management
CHAPTER 6: Information Management
CHAPTER 7: Physical Access Management
CHAPTER 8: System Development
CHAPTER 9: Business Application Management
CHAPTER 10: System Access
CHAPTER 11: System Management
CHAPTER 12: Networks and Communications
CHAPTER 13: Supply Chain Management
CHAPTER 14: Technical Security Management
CHAPTER 15: Threat and Incident Management
CHAPTER 16: Local Environment Management
CHAPTER 17: Business Continuity

Part II examines in detail the security controls intended to satisfy the defined security requirements. **Chapter 5** discusses a range of issues that encompasses both screening and application procedures as well as ongoing education and training of all employees in proper security procedures and how to

https://t.me/learningnets

conform to the organization's security policy. **Chapter 6** includes a discussion of policies for classifying information and for ensuring the privacy of information. The chapter also covers protecting documents and sensitive physical information. **Chapter 7** focuses on security issues related to physical assets. It includes equipment management and mobile device management. **Chapter 8** focuses on development activities for business applications. It includes system development management and the system development life cycle. **Chapter 9** deals with how to incorporate security controls into business applications (including specialized controls for web browser-based applications) to protect the confidentiality and integrity of information when it is input to, processed by, and output from these applications. The chapter also covers end-user applications and user-generated data, such as spreadsheets and databases. **Chapter 10** focuses on controlling access to applications, devices, systems, and networks. It includes access management and customer access issues. **Chapter 11** covers availability and security issues related to the configuration and maintenance of all IT systems in the organization. **Chapter 12** includes discussion of network management plus security measures associated with email and messaging. **Chapter 13** includes external supplier management and cloud computing services. **Chapter 14** includes technical security infrastructure and cryptography. **Chapter 15** deals with planning for and reacting to threats. It includes cybersecurity resilience and incident management. **Chapter 16** covers issues related to documenting and managing individual local environments within an organization. The chapter also deals with physical and environmental security. **Chapter 17** deals with the important topic of business continuity.

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Chapter 5

People Management

So estimable a young man! I assure you that after a few months' training he was an admirable assistant.

—*The Adventure of the Golden Pince-Nez*, Sir Arthur Conan Doyle

Learning Objectives

After studying this chapter, you should be able to:

- Describe the key security considerations in the three phases of the employment life cycle.
- Explain the four phases in the cybersecurity learning continuum.
- Present an overview of people management best practices.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) uses the term *people management* to refer to all aspects of security related to the behavior of employees and others who have access to the organization's information and systems. As many security experts have pointed out, superb technical solutions for ensuring security are bound to fail if employees do not understand their security responsibilities and are trained and motivated to fulfill those responsibilities.

Broadly speaking, this topic encompasses two areas. The first has to do with what could be called the employment life cycle: the relationship of the individual to the organization prior to employment, during employment, and at and after employment termination. The SGP refers to this area as *human resource security*. The other area has to do with the security-related training of employees, both in terms of general security awareness, as well as in terms of the use of IT assets. The SGP refers to this area as *security awareness/education*. These topics are covered in the first two sections of this chapter, followed by a review of best practices.

https://t.me/learningnets

5.1 Human Resource Security

Sound security practice dictates that information security requirements be embedded into each stage of the employment life cycle, specifying security-related actions required during the induction of each individual, the employee's ongoing management, and termination of his or her employment. Human resource security encompasses all security aspects involving employees:

- Hiring new employees
- Training employees
- Monitoring employee behavior
- Handling employee departure/termination

Especially important is the management of personnel with privileged user access to information and IT assets.

It is important for executive management—and indeed for all employees—to understand that cybersecurity is not exclusively—or even primarily—a technical challenge to be relegated to the work of IT and security professionals. As the Council on CyberSecurity points out in its *Cybersecurity Workforce Handbook* [COCS14], cybersecurity is similar to health and safety considerations, in which the actions of each employee affect the health and safety of everyone. In the case of cybersecurity, the actions of any one employee can compromise security for the entire organization. Technical fixes cannot remove vulnerabilities inherent in the workforce itself, including social engineering (such as emails with malicious links), poor credential management (such as weak or unprotected passwords), and use of insecure or poorly configured devices and applications (such as connecting "dirty" thumb drives or installing applications from unverified websites).

Thus, all employees, through awareness training, should learn basic security practice. Fortunately, many of the tasks associated with this effort are not onerous. Rather, there are some basic tasks that every employee can perform to ensure good cyber hygiene.

Security problems caused by employees fall into two categories: non-malicious and malicious. Some people unwittingly aid in the commission of security incidents by failing to follow proper procedure, by forgetting security considerations, and by not understanding what they are doing. If an organization does not have effective awareness and training programs, a problem could occur because an employee was never told what constitutes proper procedure in terms of security. Such behavior does not involve a motive to cause harm. It may be either accidental, when there is no decision to act inappropriately, or it may be negligent, when there is a conscious decision to act inappropriately. As an example of the latter case, someone may take a

https://t.me/learningnets

shortcut to increase productivity or simply to avoid hassle but might feel that he or she can do so without causing a security incident.

Other people knowingly violate controls and procedures to cause or aid in security incidents. The security problems caused by such persons can exceed those caused by outsiders, as employees with privileged access are the ones who know the controls and know what information of value may be present.

Security in the Hiring Process

ISO 27002, *Code of Practice for Information Security Controls*, lists the following security objective of the hiring process: to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Although this section is primarily concerned with employees, the same considerations apply to contractors and third-party users.

Background Checks and Screening

From a security viewpoint, hiring presents management with significant challenges. In the *Computer Security Handbook*, Kabay and Robertson [KABA14] point out that growing evidence suggests that many people inflate their resumes with unfounded claims. Compounding this problem is the increasing reticence of former employers. Employers may hesitate to give poor references for incompetent, underperforming, or unethical employees for fear of a lawsuit if their comments become known and an employee fails to get a new job. On the other hand, a favorable reference for an employee who subsequently causes problems at his or her new job may invite a lawsuit from the new employer. As a consequence, a significant number of employers have a corporate policy that forbids discussing a former employee's performance in any way, positive or negative. The employer may limit information to the dates of employment and the title of the position held.

Despite these obstacles, employers must make a significant effort to do background checks and otherwise screen applicants. Of course, such checks are done to ensure that the prospective employee is competent to perform the intended job and poses no security risk. In addition, employers need to be cognizant of the concept of "negligent hiring" that applies in some jurisdictions. In essence, an employer may be held liable for negligent hiring if an employee causes harm to a third party (individual or company) while acting as an employee.

General guidelines for checking applicants include the following:

- Ask an applicant for as much detail as possible about employment and educational history. The more detail that is provided, the more difficult it is for the applicant to lie consistently.

https://t.me/learningnets

- Investigate the accuracy of the applicant's details to a reasonable extent.
- Arrange for experienced staff members to interview candidates and discuss discrepancies.

For highly sensitive positions, more intensive investigation is warranted. The *Information Technology Security Handbook* [SADO03] gives the following examples of measures that may be warranted in some circumstances:

- Have an investigation agency do a background check.
- Get a criminal record check of the individual.
- Check the applicant's credit record for evidence of large personal debt and inability to pay it. Discuss problems, if you find them, with the applicant. People who are in debt should not be denied jobs: If they are, they will never be able to regain solvency. At the same time, employees who are under financial strain may be more likely to act improperly.
- Consider conducting a polygraph examination of the applicant (if legal). Although polygraph examinations are not always accurate, they can be helpful if you have a particularly sensitive position to fill.
- Ask the applicant to obtain bonding for his or her position.

For many employees, these steps are excessive. However, an employer should conduct extra checks of any employee who will be in a position of trust or privileged access—including maintenance and cleaning personnel.

In addition, after employment commences, managers should remain alert to changes in employees' personal circumstances that could increase incentives for system misuse or fraud.

Employment Agreements

As part of their contractual obligation, employees should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. The agreement should include a confidentiality and non-disclosure agreement that spells out specifically that the organization's information assets are confidential unless classified otherwise and that the employee must protect that confidentiality. Confidentiality agreements put all parties on notice that the organization owns its information, expects strict confidentiality, and prohibits information sharing except for that required for legitimate business needs. The agreement should also reference the organization's security policy and indicate that the employee has reviewed and agrees to abide by the policy.

https://t.me/learningnets

Job Descriptions

The Federal Financial Institutions Examination Council [FFIE02] suggests that job descriptions be designed to increase accountability for security. Management can communicate general and specific security roles and responsibilities for all employees within their job descriptions. Management should expect all employees, officers, and contractors to comply with security and acceptable use policies and protect the institution's assets, including information. The job descriptions for security personnel should describe the systems and processes they will protect and the control processes for which they are responsible. Management can take similar steps to ensure that contractors and consultants understand their security responsibilities as well.

directory server
Manages user identity and authorization data in a directory format.

A key aspect of clarifying the security responsibilities attached to a particular job description is to specify the cybersecurity tasks associated with each type of job. Figure 5.1, based on a figure in the *Cybersecurity Workforce Handbook* [COCS14], lists tasks that must be performed by everyone in the enterprise, with additional tasks assigned to those with increased responsibility for data and systems.

whitelist
A list of discrete entities, such as hosts or applications, that are known to be benign and are approved for use within an organization and/or information system.

application whitelisting
A process that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.

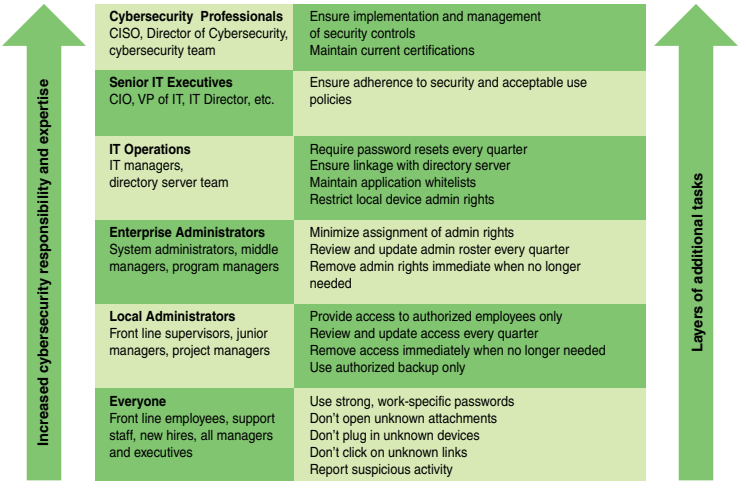


FIGURE 5.1 Security-Related Tasks by Job Description

During Employment

ISO 27002 lists the following security objective with respect to current employees: to ensure that employees and contractors are aware of and fulfill their information security responsibilities. Specifically, employees and contractors should:

- Be aware of information security threats and concerns
- Be aware of their responsibilities and liabilities with regard to information security

https://t.me/learningnets

- Be equipped to support organizational security policy in the course of their normal work

Two essential elements of personnel security during employment are (1) comprehensive security policy and acceptable use documents and (2) an ongoing awareness and training program for all employees. These are covered in Chapter 4, "Security Management," and Section 5.2, respectively.

In addition to enforcing the security policy in a fair and consistent manner, there are certain principles that need to be followed for personnel security:

- **Least privilege:** Give each person the minimum access necessary to do his or her job. This restricted access is both logical (access to accounts, networks, programs) and physical (access to computers, backup tapes, and other peripherals). If every user has accounts on every system and has physical access to everything, then all users are roughly equivalent in their level of threat.
- **Separation of duties:** Carefully separate duties so that people involved in checking for inappropriate use are not also capable of perpetrating such inappropriate use. For example, one individual should not have overlapping security access and audit responsibilities. In that case, the individual can violate security policy and cover up any audit trail that would reveal the violation.
- **Limited reliance on key employees:** It is unavoidable that some employees are key to the operation of an organization, which creates risk. Therefore, organizations should have written policies and plans established for unexpected illness or departure. As with systems, redundancy should be built into the employee structure. There should be no single employee with unique knowledge or skills. Chapter 17, "Business Continuity," deals with this topic in more detail.
- **Dual operator policy:** In some cases, it may be possible to define specific tasks that require two people. A similar policy is two-person control, which requires that two employees approve each other's work.
- **Mandatory vacations:** Mandatory vacation policies help expose employees involved in malicious activity, such as fraud or embezzlement. As an example, employees in positions of fiscal trust, such as stock traders or bank employees, are often required to take an annual vacation of at least five consecutive workdays.

Termination of Employment

ISO 27002 lists the following security objective with respect to termination of employment: to protect the organization's interests as part of the process of changing or terminating employment.

https://t.me/learningnets

The termination process is complex and depends on the nature of the organization, the status of the employee in the organization, and the reason for departure. From a security point of view, the following actions are important:

- Removing the person's name from all lists of authorized access to applications and systems
- For IT personnel, ensuring that no rogue admin accounts were created
- Explicitly informing guards that the ex-employee is not allowed into the building without special authorization by named employees
- Removing all personal access codes
- If appropriate, changing lock combinations, reprogramming access card systems, and replacing physical locks
- Recovering all assets, including employee ID, disks, documents, and equipment (assets that should have been documented when provided to the employee)
- Notifying, by memo or email, appropriate departments so that they are aware of the change in employment status
- If appropriate, escorting the ex-employee off the premises

5.2 Security Awareness and Education

A critical element of an information security program is the security awareness and training program. It is the means for disseminating security information to all employees, including IT staff, IT security staff, and management, as well as IT users and other employees. A workforce that has a high level of security awareness and appropriate security training for each individual's role is as important as, if not more important than, any other security countermeasure or control.

Two key National Institute of Standards and Technology (NIST) publications, SP 800-16, *A Role-Based Model for Federal Information Technology/Cybersecurity Training*, and SP 800-50, *Building an Information Technology Security Awareness and Training Program*, are valuable resources in this area, and this section draws on both. SP 800-50 works at a higher strategic level and discusses how to build and maintain an information security awareness and training program; SP 800-16 addresses a more tactical level and discusses the awareness–training–education continuum, role-based training, and course content considerations. Both publications define and describe a cybersecurity learning continuum that depicts a progression of learning across the spectrum of roles throughout the organization, consisting of four phases (see Figure 5.2).

https://t.me/learningnets

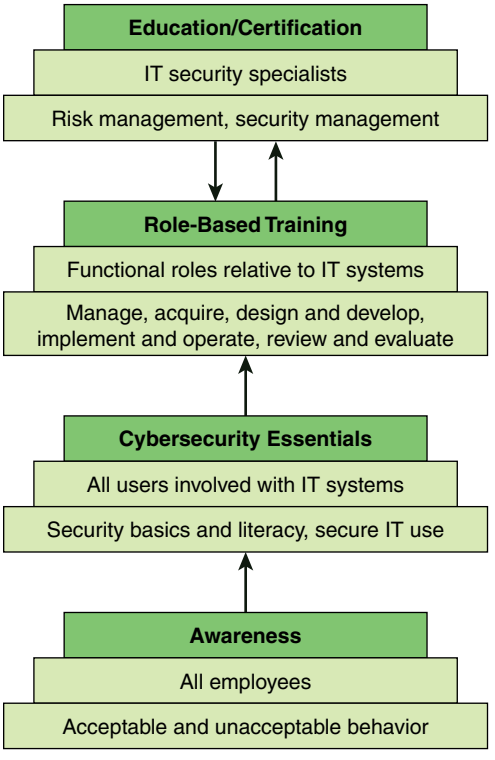


FIGURE 5.2 Cybersecurity Learning Continuum

The four phases are as follows:

- **Awareness:** A set of activities that explains and promotes security, establishes accountability, and informs the workforce of security news. Participation in security awareness programs is required for all employees.
- **Cybersecurity essentials:** Intended to develop secure practices in the use of IT resources. This level is needed for those employees, including contractor employees, who are involved in any way with IT systems. It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.
- **Role-based training:** Intended to provide knowledge and skills specific to an individual's roles and responsibilities relative to information systems. Training supports competency development and helps personnel understand and learn how to perform their security roles.
- **Education/certification:** Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technologi-

https://t.me/learningnets

Security Awareness

security awareness

The extent to which staff understand the importance of information security, the level of security required by the organization, and their individual security responsibilities.

Because all employees have security responsibilities, all employees must have suitable awareness training. Awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness is a program that continually pushes the security message to users in a variety of formats. Note that a security awareness program must reach all employees, not just those with access to IT resources. Such topics as physical security, protocols for admitting visitors, social media rules, and social engineering threats are concerns with all employees.

The overall objective of the organization should be to develop a **security awareness** program that permeates to all levels of the organization and that is successful in promoting an effective **security culture**. To that end, the awareness program must be ongoing, focused on the behavior of various categories of people, monitored, and evaluated.

security culture

The extent to which staff demonstrate expected security behavior in line with their individual security responsibilities and the level of security required by the organization.

Specific goals for a security awareness program should include:

- Providing a focal point and a driving force for a range of awareness, training, and educational activities related to information security, some of which might already be in place but perhaps need to be better coordinated and more effective
- Communicating important recommended guidelines or practices required to secure information resources
- Providing general and specific information about information security risks and controls to people who need to know
- Making individuals aware of their responsibilities in relation to information security
- Motivating individuals to adopt recommended guidelines or practices
- Being driven by risk considerations (for example, assigning risk levels to different groups of individuals, based on their job function, level of access to assets, access privileges, and so on)
- Providing employees with an understanding of the different types of inappropriate behavior—such as malicious, negligent, and accidental—and how to avoid **negligent behavior** or **accidental behavior** and recognize **malicious behavior** in others
- Creating a stronger culture of security, with a broad understanding and commitment to information security
- Helping enhance the consistency and effectiveness of existing information security controls and potentially stimulating the adoption of cost-effective controls
- Helping minimize the number and extent of information security breaches, thus reducing costs directly (for example, data damaged by viruses) and indirectly (for example, reduced need to investigate and resolve breaches)

negligent behavior

Behavior that does not involve a motive to cause harm but does involve a conscious decision to act inappropriately (for example, using unauthorized services or devices to save time, increase productivity, or enable remote working).

https://t.me/learningnets

The European Union Agency for Network and Information Security (ENISA) has identified three main processes in the development of an information security awareness program [ENIS08], as shown in Figure 5.3.

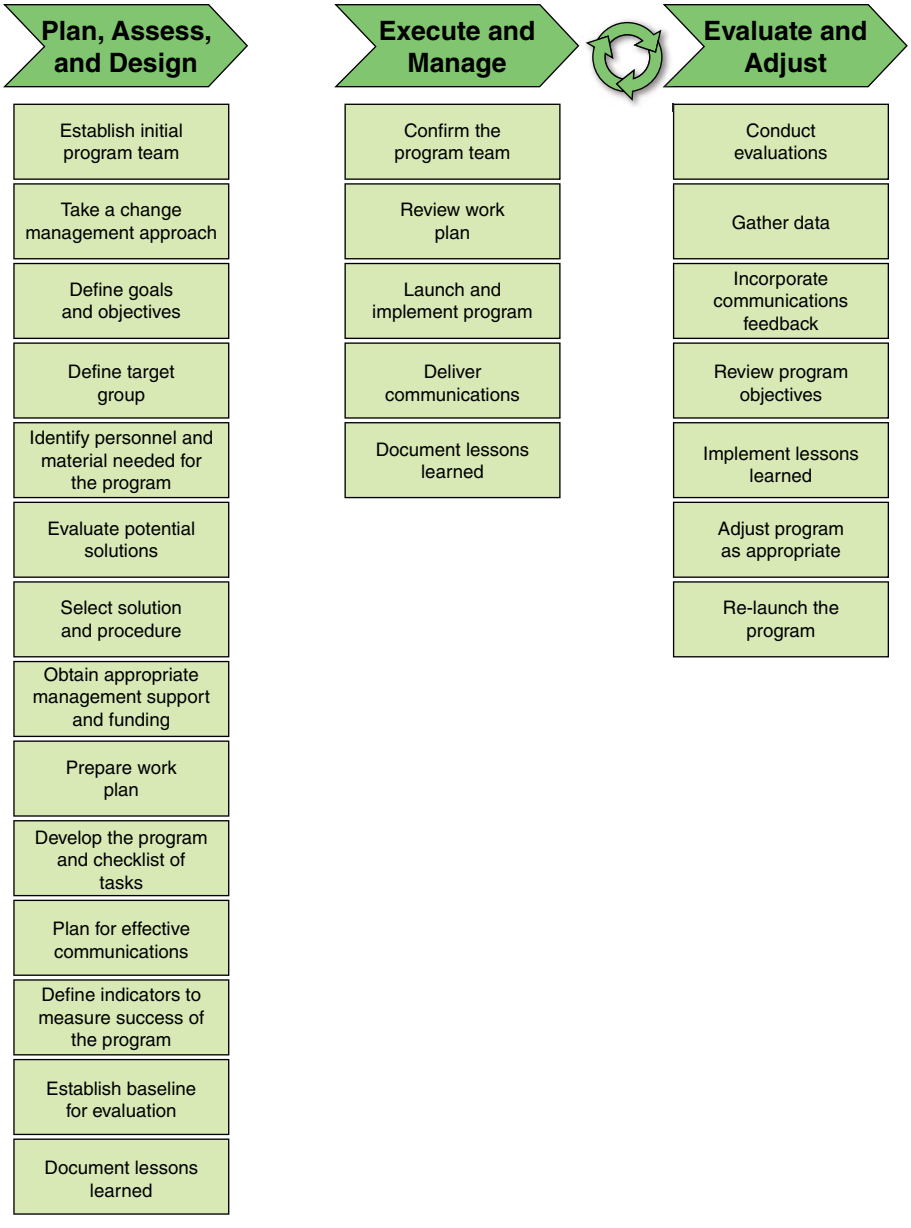


FIGURE 5.3 Security Awareness Processes

accidental behavior

Behavior that does not involve a motive to harm or a conscious decision to act inappropriately (for example, emailing sensitive information to unauthorized recipients, opening malicious email attachments, publishing personal information on publicly available servers).

malicious behavior

Behavior that involves a combination of motive to cause harm and a conscious decision to act inappropriately (for example, copying business files before taking employment with a competitor, leaking sensitive information, misusing information for personal gain).

change management

Business processes that seek to ensure that only authorized modifications are made to an item, while mitigating risk and impact to the whole. Change management is designed to minimize resistance to organizational change through involvement of key players and stakeholders.

https://t.me/learningnets

The three main processes are as follows:

- **Plan, assess, and design:** Awareness programs must be designed with the organization mission in mind. They should support the business needs of the organization and be relevant to the organization's culture and IT architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented. In the design step of the program, the awareness needs are identified, an effective awareness plan is developed, organizational buy-in is sought and secured, and priorities are established.
- **Execute and manage:** This process includes activities necessary to implement an information security awareness program. The initiative is executed and managed only when:
  - A needs assessment has been conducted
  - A strategy has been developed
  - An awareness program plan for implementing that strategy has been completed
  - Material has been developed
- **Evaluate and adjust:** Formal evaluation and feedback mechanisms are critical components of any security awareness program. The feedback mechanism must be designed to address objectives initially established for the program. Once the baseline requirements are solidified, design and implement a feedback strategy.

Awareness Program Communication Materials

At the heart of an awareness training program are the communication materials and methods used to convey security awareness. There are two options for the awareness program designer:

- Use in-house materials
- Use externally obtained materials

A well-designed program should have materials from both sources.

In-house materials that are effectively used include the following:

- **Brochures, leaflets, and fact sheets:** These short documents are used to highlight key points such as password selection and use.
- **Security handbook:** The security policy document is one candidate for a handbook. However, a document specifically geared toward awareness could be produced, covering all the security topics needed for all employees.

https://t.me/learningnets

- **Regular email or newsletter:** This communication channel is used to highlight changes either in organization security policy or outside threats, especially social engineering threats. In addition, this channel can be used to send reminders on specific topics.
- **Distance learning:** The organization can set up a set of self-paced courses that are available online.
- **Workshop and training sessions:** A block of time, such as an hour or an entire day, can be set aside, with mandatory attendance by certain categories of staff.
- **Formal classes:** Classes can be held much like workshops, but perhaps offered off-site and lasting multiple days. They could be part of a professional development program.
- **Video:** Available online or via disk, a video can cover one or more topics in depth and may be watched by individuals on their own time or on time allowed during work hours.
- **Website:** An organization security website can be established that can be updated to reflect changes, present content for multiple audiences, and link to other information.

Short communications, such as messages and emails, cover topics tailored to the role and level of access of the individual, including:

- Emphasizing the difference between **critical information** and **sensitive information**, which must be treated differently
- Providing updates on details of current and anticipated threats
- Reinforcing expected security-related activity
- Reinforcing the individual's personal responsibility for security
- Restating key security policy points
- Highlighting specific concerns related to electronic communications, such as email, blogs, and texting
- Highlighting specific security concerns related to information systems

critical information
Information that needs to be available and have integrity (for example, product prices/exchange rates, manufacturing information, medical records).

sensitive information
Information that can be disclosed only to authorized individuals (for example, product designs, merger and acquisition plans, medical records, business strategy information).

Externally obtained information and materials include the following:

- Email advisories issued by industry-hosted news groups, academic institutions, or the organization's IT security office
- Professional organizations and vendors
- Online IT security daily news websites

https://t.me/learningnets



NIST Awareness, Training, and Education (ATE) http://csrc.nist.gov/groups/SMA/ate/index.html

- Periodicals
- Conferences, seminars, and courses

The NIST Computer Security Division website's awareness, training, education, and professional development pages contain a number of links to government, industry, and academic sites that offer or sell both awareness and training materials.

Awareness Program Evaluation

Just as in other areas of security, evaluation is needed to ensure that an awareness program is meeting objectives. ENISA has developed a set of metrics that are useful for awareness program evaluation [ENIS07], as shown in Table 5.1.

TABLE 5.1 Metrics for Measuring the Success of Awareness Programs

Metric	Considerations
Number of security incidents due to human behavior	Can quickly show trends and deviations in behavior
	Can help understand root causes and estimate costs to the business
	May not be enough incidents to draw meaningful results
	May be other factors that affect the incidents
Audit findings	Generally conducted by independent and knowledgeable people who can provide third-party assurance on behaviors
	May be significant areas of awareness not reviewed
Results of staff surveys	If used before and after specific training, can be used to gauge the effectiveness of campaigns
	If sufficiently large, can provide statistical conclusions on staff behaviors
	Need to be targeted at verifying key messages
	Have to be carefully designed because staff may respond with "expected" answers and not true behaviors
Tests of whether staff follow correct procedures	Very good way of actually measuring behaviors and highlighting changes after training
	Have to be carefully planned and carried out because there could be breaches of employment and data protection laws
	Need a big enough sample if results are to be meaningful
Number of staff completing training	Need to decide what combination of classroom and computer-based training to use
	Have to consider what training to make mandatory
	May need to be tailored for different areas or regions
	May need regular and potentially costly updates

https://t.me/learningnets

Cybersecurity Essentials Program

A cybersecurity essentials program serves two purposes. Its principal function is to target users of IT systems and applications, including company-supplied mobile devices and **bring your own device (BYOD)** policies, and develop sound security practices for these employees. Secondarily, it provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.

bring your own device (BYOD)
An IT strategy in which employees, business partners, and others use their personally selected and purchased client devices to execute enterprise applications and access data and the corporate network. Typically, a BYOD policy spans smartphones and tablets, but the strategy may also be used for laptops, and it may include a subsidy.

NIST SP 800-16 defines *cybersecurity essential program* as a program that refers to an individual's familiarity with, and ability to apply, a core knowledge set that is needed to protect electronic information and systems. All individuals who use computer technology or its output products, regardless of their specific job responsibilities, must know these essentials and be able to apply them. The training at this level should be tailored to a specific organization's IT environment, security policies, and risks.

Key topics that should be covered include:

- Technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges
- Common information and computer system security vulnerabilities
- Common cyberattack mechanisms, their consequences, and motivations for use
- Different types of cryptographic algorithms
- Intrusion, types of intruders, techniques, and motivation
- Firewalls and other means of intrusion prevention
- Vulnerabilities unique to virtual computing environments
- Social engineering and its implications to cybersecurity
- Fundamental security design principles and their role in limiting points of vulnerability

Role-Based Training

Role-based training is targeted at individuals who have functional rather than user roles with respect to IT systems and applications. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, whereas awareness seeks to focus an individual's attention on an issue or a set of issues.

https://t.me/learningnets

The nature of the training depends on the role of the individual in the organization. SP 800-16 develops training recommendations based on differentiation of four major roles:

- **Manage:** The individual's job functions encompass overseeing a program or technical aspect of a security program; overseeing the life cycle of a computer system, network, or application; or having responsibilities for the training of staff.
- **Design:** The individual's job functions encompass scoping a program or developing procedures, processes, and architectures; or designing a computer system, a network, or an application.
- **Implement:** The individual's functions encompass putting programs, processes, or policies into place; or operation/maintenance of a computer system, a network, or an application.
- **Evaluate:** The individual's functions encompass assessing the effectiveness of any of the above actions.

SP 800-50 gives as an example of training an IT security course for system administrators, which addresses in detail the management controls, operational controls, and technical controls that should be implemented. Management controls include policy, IT security program management, risk management, and life cycle security. Operational controls include personnel and user issues, contingency planning, incident handling, awareness and training, computer support and operations, and physical and environmental security issues. Technical controls include identification and authentication, logical access controls, audit trails, and cryptography.

Education and Certification

An education and certification program is targeted at those who have specific security responsibilities, as opposed to IT workers who have some other IT responsibility but must incorporate security concerns.

Security education is normally outside the scope of most organization awareness and training programs. It more properly fits into the category of employee career development programs. Often, this type of education is provided by outside sources, such as college or university courses or specialized training programs.

The following are examples of such programs:

- **Global Information Assurance Certification (GIAC) Security Essentials (GSEC):** Designed for IT pros who want to demonstrate skills in IT system hands-on roles with respect to security tasks. Ideal candidates for this certification possess an understanding of information security beyond simple terminology and concepts.

https://t.me/learningnets

- **International Information System Security Certification Consortium (ISC)² Certified Information Systems Security Professional (CISSP):** Ideal candidates for this certification are information assurance pros who know how to define the information system architecture, design, management, and controls to ensure the security of business environments.
- **(ISC)² Systems Security Certified Practitioner (SSCP):** Designed for those with proven technical skills and practical security knowledge in hands-on operational IT roles. The SSCP provides confirmation of a practitioner's ability to implement, monitor, and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity, and availability.
- **Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM):** For candidates who have an inclination toward organizational security and want to demonstrate the ability to create a relationship between an information security program and broader business goals and objectives. This certification ensures knowledge of information security and development and management of an information security program.
- **SANS computer security training and certification:** The SANS Institute provides intensive immersion training designed to an organization's staff master the practical steps necessary for defending systems and networks against the most dangerous threats—the ones being actively exploited.

5.3 People Management Best Practices

The SGP breaks down the best practices in the People Management category into two areas and six topics and provides detailed checklists for each topic. The areas and topics are:

- **Human resource security:** The objective of this area is to embed information security into each stage of the employment life cycle, which includes assigning ownership of information (including responsibility for its protection) to capable individuals and obtaining confirmation of their understanding and acceptance.
  - **Employment life cycle:** Provides checklists of desired actions during the three main phases of the employment life cycle: incoming, active employee, and termination
  - **Ownership and responsibilities:** Outlines practices to achieve individual accountability for information and systems, provide a sound management structure for individuals running or using them, and give their owners a vested interest in their protection

https://t.me/learningnets

- **Remote working:** Elaborates on the principle that individuals working in remote environments (for example, in locations other than the organization's premises) should be subject to authorization; protect computing devices and the information they handle against loss, theft, and cyber attack; be supported by security awareness material; and employ additional controls when traveling to high-risk countries or regions

- **Security awareness/education:** The objective of this area is to maintain a comprehensive, ongoing security awareness program to promote and embed expected security behavior in all individuals who have access to the organization's information and systems.
  - **Security awareness program:** Outlines the specific activities that should be undertaken, such as a security awareness program, to promote and embed expected security behavior in all individuals who have access to the organization's information and systems
  - **Security awareness messages:** Discusses topics that can be addressed in messages, tailored to the role and level of access of the individual
  - **Security education/training:** Lists key components of an education and training program

5.4 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

accidental behavior
application whitelisting
bring your own device (BYOD)
change management
critical information
directory server
least privilege
malicious behavior
negligent behavior
remote working
security awareness
security culture
sensitive information
separation of duties
role-based training
whitelist

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. What does the term *employment life cycle* mean?
2. How can you categorize the security problems caused by employees?

https://t.me/learningnets

3. What should a company check, in general, before hiring a new employee?
4. How can a company ensure personnel security?
5. Suppose X has resigned from company Alpha. What actions should the security officer of Alpha take before relieving X from duty?
6. What are the four phases of the cybersecurity learning continuum?
7. What should be the goals for a security awareness program?
8. What are some of the tools used to impact awareness training?
9. What does the term BYOD stand for, and what does it mean? Cite some challenges it imposes to an organizations security.
10. What topics should an ideal cybersecurity program include?
11. What measures should an organization take to ensure security while giving remote working rights to an employee?
12. Differentiate between malicious behavior, negligent behavior, and accidental behavior.

5.5 References

COCS14: Council on CyberSecurity, *Cybersecurity Workforce Handbook: A Practical Guide to Managing Your Workforce.* 2014. http://pellcenter.org/tag/council-on-cybersecurity/.

ENIS07: European Union Agency for Network and Information Security (ENISA), *Information Security Awareness Initiatives: Current Practice and the Measurement of Success.* July 2008. https://www.enisa.europa.eu.

ENIS08: European Union Agency for Network and Information Security (ENISA), *The New Users' Guide: How to Raise Information Security Awareness.* July 2008. https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

FFIE02: Federal Financial Institutions Examination Council, *Information Security.* December 2002.

KABA14: Kabay, M., & Robertson, B., "Employment Practices and Policies." In Bosworth, S., Kabay, M., & Whyne, E. (Eds.), *Computer Security Handbook.* Hoboken: NJ: Wiley, 2014.

SADO03: Sadowsky, G., et al., *Information Technology Security Handbook.* Washington, DC: The World Bank, 2003. http://www.infodev.org/articles/information-technology-security-handbook.

https://t.me/learningnets

Chapter 6

Information Management

Polonius: What do you read, my lord?

Hamlet: Words, words, words.

—*Hamlet*, William Shakespeare

Learning Objectives

After studying this chapter, you should be able to:

- Explain the steps involved in information classification.
- Understand the requirements for information labeling.
- Present an overview of threats to privacy.
- Present an overview of the General Data Protection Regulation.
- Discuss the differences between document management and records management.
- Present an overview of the considerations involved in protecting sensitive physical information.
- Present an overview of information management best practices.

The area of information management, according to the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP), encompasses four topics, all of which are covered in this chapter:

https://t.me/learningnets

- **Information classification and handling:** Deals with methods of classifying and protecting an organization's information assets
- **Privacy:** Is concerned with threat, controls, and policies related to the privacy of personally identifiable information (PII)
- **Document and records management:** Is concerned with the protection and handling of the documents and records maintained by an organization
- **Sensitive physical information:** Covers specific issues related to the security of information assets in physical form

6.1 Information Classification and Handling

A necessary preliminary step to the development of security controls and policies for protecting information is that all the information assets of the organization must be classified according to their importance and according to the impact of security breaches involving the information. In addition, an organization needs to have clear procedures for ensuring that the link between a given type of information and its classification is maintained throughout the life cycle of the information and that procedures designate how the information is handled. ISO 27001, *ISMS Requirements*, puts all these requirements under the generic security control category of information classification, with the following requirements:

- **Classification of information:** The classification scheme should take into account legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.
- **Labeling of information:** The organization should develop and implement an appropriate set of procedures for information labeling in accordance with the information classification scheme.
- **Handling of assets:** Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme.

This section examines these three activities.

Information Classification

It is useful to view information classification and handling in the overall context of risk management. National Institute of Standards and Technology (NIST) SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*,

https://t.me/learningnets

defines a risk management framework that views the risk management process as consisting of six steps (see Figure 6.1):

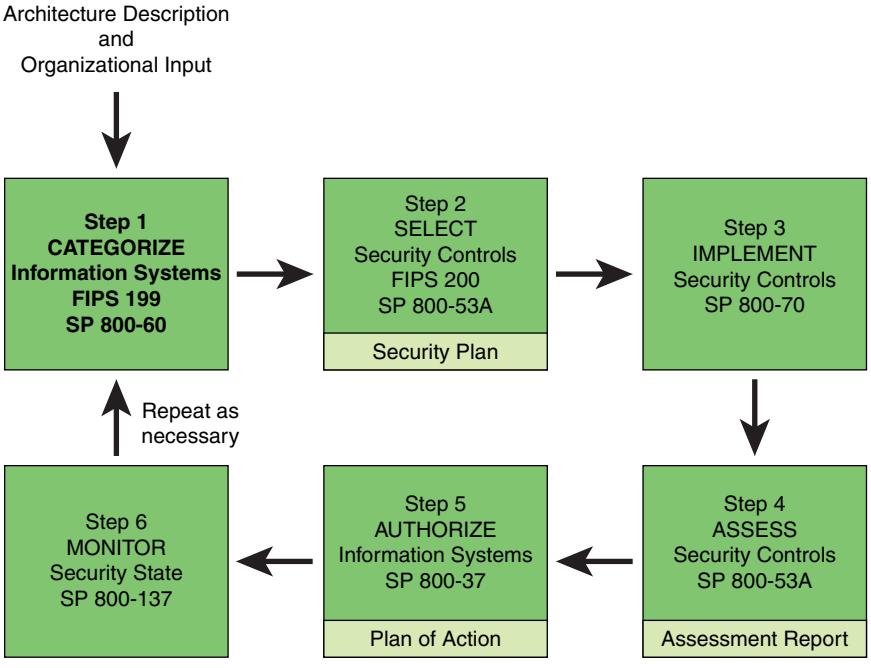


FIGURE 6.1 NIST Risk Management Framework

1. **Categorize:** An organization needs to identify the information to be transmitted, processed, or stored by the system and define applicable levels of information categorization based on an impact analysis. The handling and safeguarding of PII should be considered. The purpose of the categorization step is to guide and inform subsequent risk management processes and tasks by determining the adverse impact or consequences to the organization with respect to the compromise or loss of organizational assets—including the confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.
2. **Select:** An organization needs to select an initial set of baseline security controls for the system based on the security categorization as well as tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
3. **Implement:** An organization needs to implement security controls and document how the controls are employed within the system and its environment of operation.

https://t.me/learningnets

4. **Assess:** An organization needs to assess the security controls using appropriate assessment procedures. It must also determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to meeting the security requirements for the system.
5. **Authorize:** Management officially authorizes a system to operate or continue to operate based on the results of the security control assessment. This decision is based on a determination of the risk to organizational operations and assets resulting from the operation of the system and the determination that this risk is acceptable.
6. **Monitor:** An organization needs to continuously monitor security controls to ensure that they are effective over time as changes occur in the system and the environment in which the system operates. This includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

One of the inputs to the categorize step consists of architecture considerations. These considerations include:

- **Information security architecture:** Recall from Chapter 2, "Security Governance," that this is defined as a description of the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
- **Mission and business processes:** This refers to what the organization does, what the perceived mission or missions are, and what business processes are involved in fulfilling the mission.
- **Information system boundaries:** These boundaries, also referred to as authorization boundaries, establish the scope of protection for organizational information systems (that is, what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes.

The other major type of input to the categorize step consists of organizational inputs, including:

- Laws, directives, and policy guidance
- Strategic goals and objectives

https://t.me/learningnets

- Priorities and resource availability
- Supply chain considerations

Before proceeding, let's distinguish some interrelated concepts that are essential to information classification:

- **Information type:** A specific category of information (for example, privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, directive, policy, or regulation.
- **Security objective:** The characteristic of security to be achieved, which typically consists of confidentiality, integrity, and availability.
- **Impact:** An adverse change to the level of business objectives achieved. Also called impact level or impact value. Typically either three (low, medium, high) or five (very low, low, medium, high, very high) levels are used.
- **Security classification:** The grouping of information into classes that reflect the value of the information and the level of protection required. Also called security categorization.

Classification provides people who deal with information with a concise indication of how to handle and protect that information. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. For example, an access control policy may dictate that access to a certain group of information is limited to personnel in certain defined roles. This approach reduces the need for case-by-case risk assessment and custom design of controls.

The way classification is approached varies from one standards body to another. ISO 27001 indicates that information is to be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. ISO 27002, *Code of Practice for Information Security Controls*, provides further guidance, stating that results of classification should indicate value of assets, depending on their sensitivity and criticality to the organization (for example, in terms of confidentiality, integrity, and availability).

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides a more precise definition of security categories, specifying the following generalized format for expressing a security category:

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}

https://t.me/learningnets

Thus, in FIPS 199, the category for an information type consists of three values. An organization may instead use a more descriptive set of terms and may make a distinction between critical and sensitive information, as discussed in Chapter 5, "People Management."

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, defines the security categorization process as consisting of four steps, as shown in Figure 6.2. The following sections examine these four steps.

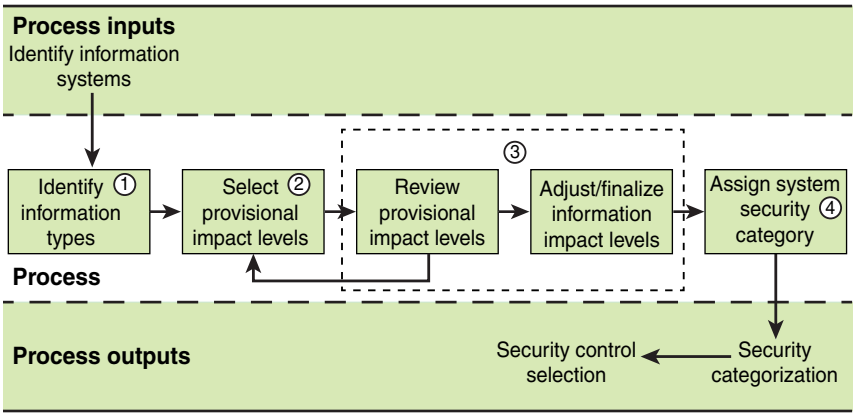


FIGURE 6.2 Security Categorization Process

Identifying Information Types

The first step of the security categorization process according to SP 800-60 is to identify the information types to be classified. The result of this step should be an information taxonomy or catalog of information types. The level of detail, or granularity, must be decided by those involved in security governance. The determination may be based on factors such as the size of the organization, its range of activities, and the perceived overall level of risk.

The identification process must cover all forms of information, including:

- Electronic, consisting of data that can be stored, transmitted, and processed
- Electronic communication, such as email and text messages
- Spoken communication, such as telephone, Skype, and teleconferencing
- Multimedia information, such as video presentations and surveillance camera recordings
- Physical information, such as paper documents

https://t.me/learningnets

SP 800-60 suggests three general organizational areas from which individual information types are defined:

- **Mission-based information:** This area encompasses types of information that relate specifically to the mission of the organization. For example, an organization in the healthcare field has information on what healthcare delivery services it provides, fee schedules, insurance arrangements, and policies for providing financial help to clients. A technology company has information about its research and development plans and goals, outside consulting arrangements, and long-range plans for new technology.
- **Services delivery support functions:** These are types of information that support the operation of the organization and relate to specific services or products offered by the organization. For example, in the area of risk management and mitigation, information types include contingency planning, continuity of operations, and service recovery.
- **Back office support functions:** These support activities enable the organization to operate effectively. SP 800-60 identifies five main groups of information types in this area:
  - Administrative management
  - Financial management
  - Human resource management
  - Information management
  - Technology management

As an example, in the information and technology management group, SP 800-60 lists system and network monitoring as an information type, with the following suggested classification:

{(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

Whatever classification scheme an organization uses, it needs to have clear definitions of the various classification levels so that all those involved in classifying information types are working with the same understanding. A useful tool in this context is the Business Impact Reference Table (BIRT; refer to Figure 3.11 in Chapter 3, "Information Risk Assessment"), which provides consistent definitions to different types of impacts and severity levels.

Selecting and Reviewing Impact Levels

The second step of the security categorization process according to SP 800-60 is to assign security impact levels for the identified information types. The worksheet in

https://t.me/learningnets

Figure 3.4 and the asset register in Figure 3.5 in Chapter 3 are examples of ways to document this process.

As an example, in the information and technology management group, SP 800-60 lists system and network monitoring as an information type, with the following suggested classification:

{(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

The third step of the security categorization process according to SP 800-60 is simply to review the provisional impact levels, allowing a range of managers and information owners to contribute to the process.

Assigning Security Categories

The final step of the security categorization process according to SP 800-60 is to assign a security classification for each information type. If the scheme suggested in SP 800-60 is used, the overall classification of an information type corresponds to its assessed impact, which is the highest of the confidentiality, integrity, and availability impacts. Otherwise, the impact information needs to be mapped into a classification scheme.

An important consideration is the naming of each classification level. The name should make sense in the context of the classification scheme's application. Classifying information types and properly naming them provide people who deal with information with a concise indication of how to handle and protect that information.

Information Labeling

A label needs to be associated with each instance of an information type so that its classification is clearly and unambiguously known. Methods are needed to ensure that a label is not separated from the information and that the content of the label is secure from unauthorized modification. The organization, for convenience and efficiency, may choose not to label non-confidential information.

radio-frequency identification (RFID)
A data collection technology that uses electronic tags attached to items to allow the items to be identified and tracked with a remote system. The tag consists of an RFID chip attached to an antenna.

For physical information types, some sort of physical label needs to be attached. This could be a readable label or bar code that adheres to the medium. In some cases, a **radio-frequency identification (RFID)** tag, which provides other security functionality, may be attached to the information medium. For information stored in electronic form, a number of techniques could be used, including using electronic watermarking, labeling headers and footers, embedding labels in metadata (such as document properties), and using filename conventions. Digital signatures can be used in electronic communications.

https://t.me/learningnets

Information Handling

Information handling refers to processing, storing, communicating, or otherwise handling information consistent with its classification.

ISO 27002 lists the following relevant considerations:

- Access restrictions supporting the protection requirements for each level of classification
- Maintenance of a formal record of the authorized recipients of assets
- Protection of temporary or permanent copies of information to a level consistent with the protection of the original information
- Storage of IT assets in accordance with manufacturers' specifications
- Clear marking of all copies of media for the attention of the authorized recipient

Wherever possible, use automated tools to enforce the proper handling of information based on its classification level. These can be special-purpose tools for the following:

data loss prevention (DLP)

A set of technologies and inspection techniques used to classify information content contained within an object—such as a file, an email, a packet, an application, or a data store—while at rest (in storage), in use (during an operation), or in transit (across a network). DLP tools also have the ability to dynamically apply a policy—such as log, report, classify, relocate, tag, and encrypt—and/or apply enterprise data rights management protections.

- Labeling information easily, correctly, and consistently
- Binding classification details to information (for example, using metadata, XML attributes, or similar techniques)
- Communicating their protection requirements effectively

An organization can also take advantage of broader information management tools, such as a document management system (DMS) or a records management system (RMS); these are discussed in Section 6.3.

The automated tools should facilitate integration with other security tools, such as encryption and digital signature modules and **data loss prevention (DLP)** packages.

6.2 Privacy

ISO 7498-2, *Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*, defines *privacy* as the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. The U.S. National Research Council's report *At the Nexus of Cybersecurity and Public Policy* [CLAR14] indicates that in the context of information, the term *privacy* usually refers to making ostensibly private information

https://t.me/learningnets

about an individual unavailable to parties who should not have that information. Privacy interests attach to the gathering, control, protection, and use of information about individuals.

In the context of cybersecurity, there is concern with the privacy of PII (as opposed, say, to video surveillance). Examples of information that might be considered PII are as follows:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number (PIN), such as Social Security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, or financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of a person's face or other distinguishing characteristic), X-rays, fingerprints, or other biometric image or template data (for example, retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (for example, date of birth, place of birth, race, religion, weight, activities, geographic indicators, employment information, medical information, education information, financial information)

The two concepts of privacy and information security are closely related. On the one hand, the scale and interconnectedness of personal information collected and stored in information systems has increased dramatically, motivated by law enforcement, national security, and economic incentives. Economic incentives have perhaps been the main driving force. In a global information economy, it is likely that the most economically valuable electronic asset is aggregation of information on individuals [JUDY14]. On the other hand, individuals have become increasingly aware of the extent to which government agencies, businesses, and even Internet users have access to their personal information and private details about their lives and activities.

https://t.me/learningnets

Although security and privacy are related, they are not equivalent. Cybersecurity, or information security, protects privacy. For example, an intruder seeking ostensibly private information (for example, personal emails or photographs, financial or medical records, phone calling records) may be stymied by good cybersecurity measures. In addition, security measures can protect the integrity of PII and support the availability of PII. However, *At the Nexus of Cybersecurity and Public Policy* [CLAR14] points out that certain measures taken to enhance cybersecurity can also violate privacy. For example, some proposals call for technical measures to block Internet traffic containing malware before it reaches its destination. But to identify malware-containing traffic, the content of all in-bound network traffic must be inspected. But inspection of traffic by any party other than its intended recipient is regarded by some as a violation of privacy because most traffic is in fact malware-free. Under many circumstances, inspection of traffic in this manner is also a violation of law.

Figure 6.3, from NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, shows a non-proportional representation of the relationship between the privacy and security domains. While some privacy concerns arise from unauthorized activity, privacy concerns also can arise from authorized processing of information about individuals. Recognizing the boundaries and overlap between privacy and security is key to determining when existing security risk models and security-focused guidance may be applied to address privacy concerns—and where there are gaps that need to be filled in order to achieve an engineering approach to privacy. For instance, existing information security guidance does not address the consequences of a poor consent mechanism for use of PII, the purpose of transparency, what PII is being collected, or which changes in use of PII are permitted as long as authorized personnel are conducting the activity. Given these material distinctions in the disciplines, it should be clear that agencies cannot effectively manage privacy solely on the basis of managing security.

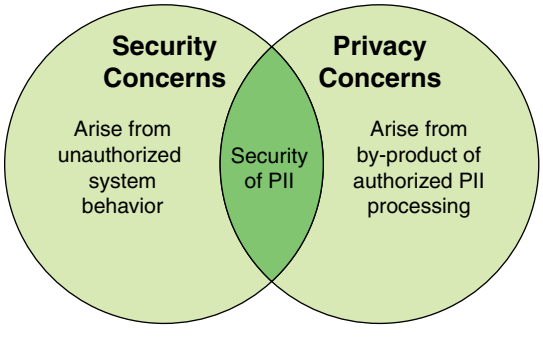


FIGURE 6.3 Relationship Between Information Security and Privacy

https://t.me/learningnets

Privacy Threats

To understand the requirements for privacy, the threats must first be identified. One of the most comprehensive lists of privacy threats is developed in Solove's *A Taxonomy of Privacy* [SOLO06]. This taxonomy describes the different kinds of activities that impinge on privacy. It consists of four basic groups of harmful activities: information collection, information processing, information dissemination, and invasion (see Figure 6.4). Each of these groups consists of different related subgroups of harmful activities.

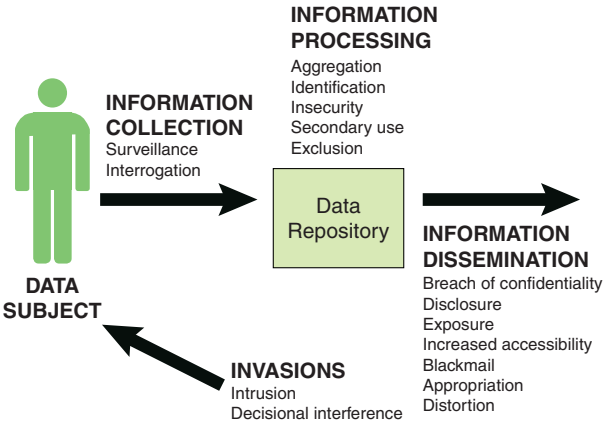


FIGURE 6.4 Potential Privacy Threats

Information collection is not necessarily harmful but can in some cases constitute a privacy threat. Two types of threat actions can occur:

- **Surveillance:** This is the watching, listening to, or recording of an individual's activities. It can be problematic and a violation of the right to privacy, especially if the target doesn't know about the surveillance.
- **Interrogation:** Interrogation is the pressuring of individuals to divulge information. For example, if certain fields in a form or in an online registration process are required in order to proceed, the individual is compelled, or at least pressured, to divulge information that he or she may prefer not to give.

Information processing refers to the use, storage, and manipulation of data that have been collected. Privacy issues relating to information processing arise from how data that have already been collected are handled and the ability to link the results back to

https://t.me/learningnets

the individuals to whom it pertains. Potential sources of privacy threats in this area include the following:

- **Aggregation:** Aggregation of data about an individual in various databases allows anyone with access to the aggregated data to learn more about an individual than could be learned from separate, and separately protected, data sets.
- **Identification:** It is possible, with sufficient data, to be able to aggregate data from various sources and use those data to identify persons who are not otherwise identified in the data sets.
- **Insecurity:** *Insecurity* refers to the improper protection and handling of PII. Identity theft is one potential consequence of insecurity. Another possible consequence is the dissemination of false information about a person, through alteration of that person's record.
- **Secondary use:** With secondary use, information about a person obtained for one purpose is used or made available for other purposes without consent.
- **Exclusion:** This is the failure to provide individuals with notice and input about their records.



Chase Bank Online Privacy Policy https://www.chase.com/digital/resources/privacy-security/privacy/online-privacy-policy

The area of information dissemination encompasses the revelation of personal information or the threat of such revelation. Potential sources of privacy threat in this area include the following:

- **Disclosure:** *Disclosure* refers to the release of true information about a person. The potential harm is damage to reputation or position in some form. For example, a website may have a privacy link at the bottom of the main page that goes to a page that states the organization's privacy policy, which is focused on disclosure issues. Typical sections of a policy include what information is collected; use of information; disclosure of information; cookies, web beacons and other tracking technologies; and user choice. Links to two examples of policies are provided in the margin.
- **Breach of confidentiality:** Solove's *A Taxonomy of Privacy* [SOLO06] distinguishes between disclosure and breach of confidentiality, defining the latter as a disclosure that involves the violation of trust in a relationship. Thus, even if a disclosure itself is not harmful, the source of the disclosure is an entity that the person has a specific expectation of trust with. An example is the unauthorized release of medical information to a third party.
- **Exposure:** Exposure involves the exposure to others of certain physical and emotional attributes about a person, such as nude photographs or a video of a surgical procedure.



Google Privacy Policy https://www.google.com/intl/en_us/policies/privacy/?fg=1

https://t.me/learningnets

- **Increased accessibility:** With increased accessibility, information that is already publicly available is made easier to access. Increased accessibility does not create a new harm but does increase the likelihood and therefore the risk.
- **Blackmail:** Blackmail involves the threat of disclosure. Ransomware is an example of blackmail in the cybersecurity context.
- **Appropriation:** Appropriation involves the use of a person's identity or personality for the purpose of another. This is not identity theft, in that the offender is not claiming to be the victim. Rather, the offender makes use of the image or other identifying characteristic for some purpose, such as advertising, not authorized by the victim.
- **Distortion:** Distortion is the manipulation of the way a person is perceived and judged by others; it involves the victim being inaccurately exposed to the public. Distortion is achieved by modifying records associated with an individual.

The fourth area of privacy threats is referred to as *invasions*, and it involves impingements directly on the individual. Potential sources of privacy threat in this area include the following:

- **Intrusion:** In general terms, intrusion involves incursions into a person's life or personal space. In the context of cybersecurity, intrusion relates to penetrating a network or a computer system and achieving some degree of access privilege. Intrusion is a part of a variety of security threats but can also cause a privacy threat. For example, the actual intrusion, or threat of intrusion, into a personal computer can disrupt the activities or peace of mind of the personal computer user.
- **Decisional interference:** This is a broad legal concept. In terms of the present discussion, it involves the individual's interest in avoiding certain types of disclosure. To the extent that certain actions, such as registering for a government benefit, might generate data that could potentially be disclosed, the decision to perform those actions is deterred.

The preceding list of potential threats is comprehensive, and it is unlikely that any organization's set of privacy controls will attempt to address all of them. However, it is useful to have such a list in determining priorities for selecting privacy controls.

Privacy Principles and Policies

A number of international organizations and national governments have introduced standards, laws, and regulations intended to protect individual privacy. The following sections examine one standard and two regional examples.

https://t.me/learningnets

ISO 29100

ISO 29100, *Privacy Framework*, lists the following 11 privacy principles that form the bases of this international standard:

- **Consent and choice:** Enables the PII principal (the person to whom the PII relates) to exercise consent to use PII and provides an opt-out/opt-in choice.
- **Purpose legitimacy and specification:** Defines the purposes for which PII can be used with clear specification to the PII principal.
- **Collection limitation:** Limits the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).
- **Data minimization:** Minimizes the processing of PII.
- **Use, retention, and disclosure limitation:** Limits the use, retention, and disclosure (including transfer) of PII to that which is necessary in order to fulfill specific explicit and legitimate purposes.
- **Accuracy and quality:** Ensures that the PII is accurate, obtained from a reliable and verified source, and provides periodic checks of information integrity.
- **Openness, transparency, and notice:** Provides PII principals with clear and easily accessible information about the PII controller's policies, procedures, and practices with respect to the processing of PII.
- **Individual participation and access:** Gives PII principals the ability to access their PII, challenge its accuracy, and provide amendments or removals.
- **Accountability:** Adopts concrete and practical measures for PII protection.
- **Information security:** Protects PII under its authority with appropriate controls at operational, functional, and strategic levels to ensure the integrity, confidentiality, and availability of the PII and protects it against risks such as unauthorized access, destruction, use, modification, disclosure, or loss throughout the whole of its life cycle.
- **Privacy compliance:** Verifies and demonstrates that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors.

These principles include information security considerations but are much broader than that.

https://t.me/learningnets

European Union's GDPR

One of the most comprehensive initiatives is European Union's (EU's) General Data Protection Regulation (GDPR), approved by the European Parliament in 2016, with an effective enforcement date of May 2108. It is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations, both public and private, across the region approach data privacy.

Table 6.1 summarizes the key principles at the heart of the GDPR.

TABLE 6.1 Key Principles of the EU's GDPR

Principle	Description
Fair, lawful, and transparent processing	The requirement to process personal data fairly and lawfully is extensive. It includes, for example, an obligation to tell data subjects what their personal data will be used for.
Purpose limitation	Personal data collected for one purpose should not be used for a new, incompatible, purpose. Further processing of personal data for archiving, scientific, historical, or statistical purposes is permitted, subject to appropriate laws and regulations.
Data minimization	Subject to limited exceptions, an organization should only process the personal data that it actually needs to process in order to achieve its processing purposes.
Accuracy	Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
Data retention periods	Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Data subjects have the right to erasure of personal data, in some cases sooner than the end of the maximum retention period.
Data security	Technical and organizational measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.
Accountability	The controller is obliged to demonstrate that its processing activities are compliant with the data protection principles.

Kinast's *10 Key Facts Businesses Need to Note About the GDPR* [KINA16] summarizes important aspects of the GDPR that organizations that do business in Europe need to be aware of:

- The GDPR applies to all companies worldwide that process personal data of EU citizens. Any company that works with information related to EU citizens must comply with the requirements of the GDPR, making it the first global data protection law. This aspect alone contributes significantly to all companies around the world taking data privacy more seriously.

https://t.me/learningnets

- The GDPR widens the definition of personal data compared to prior EU regulations. As a result, parts of IT that have been unaffected by data protection laws in the past will need attention from businesses to ensure that they comply with the new regulation. The GDPR definition states that personal data means any information related to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- The GDPR tightens the rules for obtaining valid consent to use personal information. Having the ability to prove valid consent for using personal information is likely to be one of the biggest challenges presented by the GDPR. The GDPR states that the consent of the data subject means any freely given, specific, informed, and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
- The GDPR requires public authorities processing personal information to appoint a data protection officer (DPO), as well as other entities, when core activities require regular and systematic monitoring of data subjects on a large scale or consist of "processing on a large scale of special categories of data.
- The GDPR mandates data protection impact assessments. Data controllers must conduct assessments where privacy breach risks are high in order to minimize risks to data subjects. This means before an organization can implement projects involving personal information, it must conduct a privacy risk assessment and work with the DPO to ensure that it is in compliance as projects progress.
- The GDPR requires organizations to notify the local data protection authority of a data breach within 72 hours of discovering it. This means organizations need to ensure that they have technologies and processes in place that enable them to detect and respond to a data breach.
- The GDPR introduces the right to be forgotten. Also known as *data erasure*, the right to be forgotten entitles the data subject to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing or a data subject withdrawing consent. This means organizations must get fresh consent before they alter the way they are using the data they have collected. It also means organizations must ensure that they have the processes and technologies in place to delete data in response to requests from data subjects.

https://t.me/learningnets

- The GDPR requires that privacy be included in systems and processes by design. At its core, privacy by design calls for the inclusion of data protection from the outset of the designing of systems rather than as an addition.

The GDPR is an important landmark in the evolving integration of privacy in cybersecurity. Even organizations unaffected by this regulation should be aware of its provision and consider them in designing their own privacy controls.

U.S. Privacy Laws and Regulations

There is no single law or regulation covering privacy in the United States. Rather, a collection of federal privacy laws cover various aspects of privacy; many of them impose mandates on private organizations as well as government agencies and departments. These include:

- **The Privacy Act of 1974:** Specifies the rules that a federal agency must follow to collect, use, transfer, and disclose an individual's PII.
- **The Fair and Accurate Credit Transaction Act of 2003 (FACTA):** Requires entities engaged in certain kinds of consumer financial transactions (predominantly credit transactions) to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft.
- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA):** Requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records.
- **The Family Educational Rights and Privacy Act of 1974 (FERPA):** Designed to protect students and their families by ensuring the privacy of student educational records.
- **The Gramm–Leach–Bliley Act of 1999 (GLBA):** Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data.
- **Federal Policy for the Protection of Human Subjects:** Outlines the basic ethical principles (including privacy and confidentiality) in research involving human subjects. Published in 1991 and codified in separate regulations by 15 federal departments and agencies.
- **The Children's Online Privacy Protection Act (COPPA):** Governs the online collection of personal information from children under age 13.
- **The Electronic Communications Privacy Act:** Generally prohibits unauthorized and intentional interception of wire and electronic communications during the transmission phase and unauthorized access of electronically stored wire and electronic communications.

https://t.me/learningnets

Privacy Controls

So far, this section has looked at potential threats to privacy and a broad approach to government regulation of privacy. To counter privacy threats and comply with government laws and regulations, organizations need a set privacy controls that encompass their privacy requirements and that respond to legal requirements. A useful and comprehensive set of such controls is provided in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. The set is organized into 8 families and a total of 24 controls:

- **Authority and purpose:** This family ensures that organizations identify the legal bases that authorize a particular PII collection or activity that impacts privacy and specify in their notices the purpose(s) for which PII is collected. These controls would be embodied in a policy statement.
- **Accountability, audit, and risk management:** This family consists of controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk. It includes the following controls:
  - **Governance and privacy program:** This includes designating a chief privacy officer, monitoring national privacy laws, allocating sufficient resources for an organizationwide privacy program, developing a strategic privacy plan, and developing a privacy policy.
  - **Privacy impact and risk assessment:** This includes implementing a risk management process and conducting privacy impact assessments where appropriate.
  - **Privacy requirements for contractors and service providers:** This involves establishing and including in contracts privacy responsibilities.
  - **Privacy monitoring and auditing:** This involves monitoring and auditing privacy controls and the internal privacy policy to ensure effective implementation.
  - **Privacy awareness and training:** This involves implementing awareness programs for all employees and training for those with privacy responsibilities.
  - **Privacy reporting:** This involves developing any mandated privacy reports for regulatory bodies.
  - **Privacy-enhanced system design and development:** This involves designing information systems to support privacy by automating privacy controls.
  - **Accounting of disclosures:** This involves keeping an accurate accounting of disclosures and making it available to the person affected.

https://t.me/learningnets

- **Data quality and integrity:** The objective of this family is to ensure that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used. This control includes procedures for confirming to the greatest extent possible the quality of the PII collected or created and documenting processes to ensure integrity.
- **Data minimization and retention:** This family includes the following controls:
  - **Minimization of PII:** This involves establishing procedures to identify the minimum relevant and necessary PII.
  - **Data retention and disposal:** This involves retaining PII only as long as necessary and providing secure methods of deletion and destruction.
  - **Minimization of PII used in testing, training, and research:** This involves developing and implementing policies and procedures to minimize use of PII in testing, training, and research.
- **Individual participation and redress:** This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. It includes the following:
  - **Consent:** This involves providing means, where feasible and appropriate, for individuals to express explicit consent to the use of their PII and to be aware of and consent to all additional uses of their PII beyond the initial consent.
  - **Individual access:** This involves providing individuals the ability to have access to their PII.
  - **Redress:** This involves providing a process by which an individual can have inaccurate PII corrected.
  - **Complaint management:** This involves implementing a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.
- **Security:** This family ensures that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure. These controls are meant to supplement the organization's security controls that may be relevant to privacy. Included are the maintenance of an inventory of PII and developing a privacy incident response plan.
- **Transparency:** This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities. This includes procedures for notifying individuals of the status of their PII and dissemination of privacy program information.

https://t.me/learningnets

- **Use limitation:** This family ensures that the scope of PII use is limited to the intended purpose. This includes developing policies and procedures to limit internal access to PII to only those personnel who require and are authorized access, as well as similar policies and procedures for third parties outside the organization.

With respect to awareness and training, NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, suggests covering the following topics:

- Definition of PII
- Applicable privacy laws, regulations, and policies
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognition of a security or privacy incident involving PII
- Retention schedules for PII
- Roles and responsibilities in responding to PII-related incidents and reporting

The scope of privacy controls that an organization needs to implement depends on the extent of the organization's involvement with PII.

6.3 Document and Records Management

A specific class of information consists of documents and records. There are no standardized, universally accepted definitions in this realm, but for this context, the following definitions are appropriate:

- **Document:** A set of information pertaining to a topic, structured for human comprehension, represented by a variety of symbols, and stored and handled as a unit. A document may be modified.
- **Record:** A subclass of documents that clearly delineates terms and conditions, statements, or claims or that provides an official record. Generally a record, once created, is not modified.

https://t.me/learningnets

The following additional definitions are useful for this section:

- **Document management:** The capture and management of documents within an organization. The term originally implied only the management of documents after they were scanned into a computer. Subsequently, it became an umbrella term embracing document imaging, workflow, text retrieval, and multimedia.
- **Document management system:** Software that manages documents for electronic publishing. It generally supports a large variety of document formats and provides extensive access control and searching capabilities across networks. A document management system may support multiple versions of a document and may be able to combine text fragments written by different authors. It often includes a workflow component that routes documents to the appropriate users.
- **Records management:** The creation, retention, and scheduled destruction of an organization's sensitive or important paper and electronic records. Computer-generated reports fall into the records management domain, but traditional data processing files do not.
- **Records management system:** Software that provides tools for and aids in records management.

Table 6.2, based on the *CMS Wire* article "6 Ways Document Management and Records Management Differ" [ROE10], summarizes some key differences between document and records management.

TABLE 6.2 Differences Between Document and Records Management

Function	Document Management	Records Management
Purpose	Makes it easier for users with a shared purpose to access and manage documents. It also allows these users to collaborate on those documents.	Is concerned with identifying, storing, maintaining, and managing data that is used to describe events in an organization's work cycle that are related to statutory, regulatory, fiscal, or operational activities within the organization.
Storage	Includes the ability to access and revise, possibly with version tracking and histories.	Intended to keep records with their original format and content.
Automated processes	May include capture and storage, control of the document's life cycle, and access control.	Manages records in a consistent manner, preserving content as well as the context and structure they came from. Supports auditing of records in their original form.

https://t.me/learningnets

Function	Document Management	Records Management
Security	Provides access control, with a means of tracking who has been using a document, when it was accessed, and any changes that were made to the document.	Provides more stringent security, including authentication and data integrity.
Disposal	The disposal of documents in a document management system occurs when the life cycle of the document has been complete and is no longer needed in the business process. Disposal can consist of simple destruction or turning the documents into records. The decision to turn a document into a record depends on the need of the company and whether there are legal requirements to hold on to the documents.	The destruction of records is generally regulated by law with strict procedures so that the information contained in them will not be disclosed.

Document Management

Document management is a key business function because of the importance of documents to the operation of an organization. Table 6.3, from the *MIS Quarterly* article "Electronic Document Management: Challenges and Opportunities for Information Systems Managers" [SPRA95], lists some of the important roles and purposes of documents within an organization.

TABLE 6.3 Roles of Documents

Role	Examples
To record or to document contracts and agreements	Employment contracts, maintenance agreements, consulting contracts, purchase agreements, leases, mortgages, loans, and so on
To record policies, standards, and procedures	Procedure manuals, standards specifications, instruction handbooks, executive memos and letters that state corporate policy, and so on
To represent a view of reality at a point in time (reports and plans)	Status reports, problem analyses, operational reports, staff recommendations, budgets, strategic plans, and so on
To create an image or impression	Annual reports, marketing brochures, TV or radio commercials, and so on
To generate revenue as a product	A book for sale by a publisher, a report by a consulting firm to be sold to its client, a news item from a wire service, a reference from a bibliographic service, and so on
To support revenue by adding value to a product	A user's manual for a car or an appliance or a software product, a warranty form, a catalog, a discount coupon for another purchase, and so on

https://t.me/learningnets

Role	Examples
To act as a mechanism for communication and interaction among people and groups	Memos, letters, presentations, email messages, minutes of meetings, and so on
To act as a vehicle for organizational process	Orders, invoices, approval letters, most business forms, and so on
To provide a discipline for capture and articulation of concepts and ideas	Nearly all the kinds of documents that carry concepts and ideas

Although the focus of document management and of document management systems is the ease of creation and use of documents, security must be an integral aspect. One key element is the management of the document life cycle, including creation, categorization, storage, retrieval, modification, and destruction. Security mechanisms need to be implemented to ensure that security objectives are met during each stage of the document life cycle.

An important security policy consideration with document management is document retention. Classify documents by type with respect to legal and regulatory requirements for retention. Define a process for third-party access to documents. And specify the retention period for each class of documents. Reclassify any documents as records that are to be retained indefinitely after they are no longer available for modification.

Figure 6.5 illustrates a typical document management life cycle.

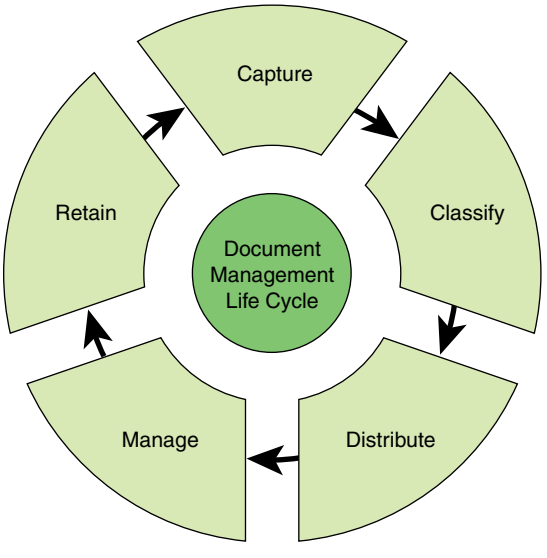


FIGURE 6.5 Document Management Life Cycle

https://t.me/learningnets

It consists of the following phases:

- **Capture:** Capture documents from various sources and place them in the document management system.
- **Classify:** Classify a document to give it business context and to allow metadata to be assigned.
- **Distribute:** Allow documents to continue through the life cycle, gathering additional information to be reviewed and approved.
- **Manage:** Present documents to users through various interfaces and applications to make the delivery as seamless as possible.
- **Retain:** Keep the document for a period defined in the classification before archiving or destruction.

As in other areas, an organization should develop acceptable use policies and awareness programs with respect to documents.

Records Management

Records management is a vital business function that requires stronger security measures than those for document management. You should treat as records those documents that have significant business value or are within the scope of relevant laws or regulations. A general process for records management is shown in Figure 6.6.

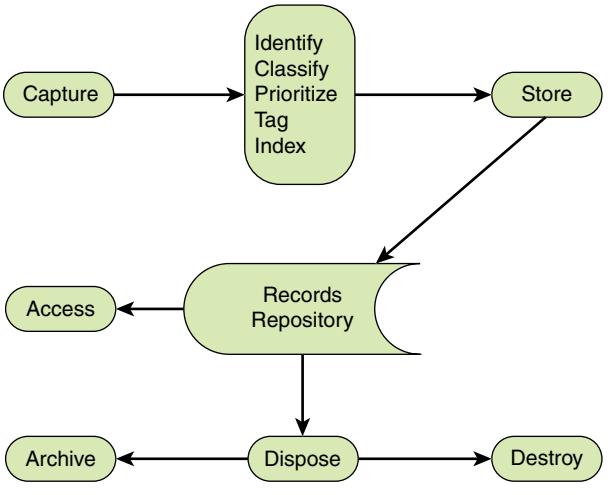


FIGURE 6.6 Records Management Functions

https://t.me/learningnets

Important guidelines for securing records include:

- Develop clear and detailed policies that define what documents should be classified as records.
- Store only a single instance of the document, whether it is physical or electronic.
- Define access restrictions as tightly as is reasonable.
- Monitor each record to ensure compliance with the organization's records retention policy.
- Ensure secure destruction of a record or secure archival of the record when the retention period has expired.

The *Information Security Guide* developed by the Higher Education Information Security Council (HEISC), suggests the following considerations for developing a records management program [HEIS14]:

- Establish a strategic planning group that includes top managers/executives to support the program.
- Write and communicate a directive on the objectives of the program, which should link to organizational goals.
- Identify a records manager to oversee all aspects of the program, including ongoing management and use of internal personnel or outside consultants.
- Write a policy statement identifying purpose, responsibility, objectives, and so on.
- Determine staffing and organizational structure for overseeing the program's day-to-day operations.
- Conduct a preliminary file purge of non-records from filing systems.
- Complete a records inventory.
- Develop and implement a retention schedule.
- Protect the vital records of the organization.
- Develop a records management manual with defined policies and procedures.
- Implement filing standards throughout.
- Identify a process for managing inactive records in a low-cost space.
- Implement forms management and reports management programs.

https://t.me/learningnets

- Automate records management where it makes sense to do so.
- Make records management a high priority.

A key aspect of records management is the retention and disposition policy. The life cycle of records is distinguished in three stages:

- **Active:** Currently used to support the organization's functions and reporting requirements. Generally, active records are those that are referred to often during the regular course of business.
- **Semi-active:** Records that are no longer needed to carry out current activities but must still be retained to meet the organization's administrative, fiscal, legal, or historical requirements. These records can be stored in less accessible storage.
- **Inactive:** Records that are no longer required to carry out the administrative or operational functions for which they were created and that are no longer retrieved or accessed. Such records can either be archived or destroyed.

6.4 Sensitive Physical Information

Sensitive information held in physical form (that is, sensitive physical information) needs to be protected against corruption, loss, and unauthorized disclosure. Examples of sensitive physical information are blank checks, bonds, and printouts of documents such as personal information, financial projections, business plans, and product designs.

COBIT 5 summarizes the requirement for protection of sensitive physical information as follows: Provide adequate, specific information security measures for data and information that exist in non-digital forms, including documents, media, facilities, physical perimeter, and transit. COBIT 5 lists the following as supporting technologies:

- Closed-circuit television (CCTV)
- Locks
- Alarms
- Access control
- Vaulting
- Intelligence reports
- First responder interfaces

https://t.me/learningnets

- Facilities management solutions
- Fire protection systems
- Time locks
- Physical access solutions

The key issues involved with securing physical information throughout its life cycle include the following:

- **Identify and document:** Each item of physical information needs to be identified properly and its existence documented.
- **Classification:** Every physical document or other type of media (for example, DVD) should be classified using the same security categories used for all other organization assets.
- **Label:** The appropriate security classification label must be affixed to or incorporated into the document itself.
- **Storage:** Secure storage is needed. This may be a safe, a secure area of the facility, or other physical means of restricting and controlling access.
- **Secure transport:** If sensitive information is to be sent by a third party, such as a courier or shipping service, policies and procedures must be in place to ensure that this is done securely. Employees who carry documents must be given guidance and the technical means needed to maintain security.
- **Disposal:** A retention and disposal policy is needed, and secure means of destroying physical information must be followed.

6.5 Information Management Best Practices

The SGP breaks down the best practices in the information management category into two areas and four topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Information classification and privacy:** This area includes the following topics:
  - **Information classification and handling:** The objective for this topic is to develop an information classification scheme that provides consistent classification of all forms of information, including electronic, physical, and spoken. The scheme should be supported by information handling

https://t.me/learningnets

guidelines to help protect information against corruption, loss, and unauthorized disclosure.

- **Information privacy:** This topic deals with the need for implementing policies and security controls for the handling of PII. The SGP recommends a separate privacy policy document and an acceptable use document. Methods are required for dealing with breaches, including detection, response, and notification.

- **Information protection:** This area includes the following topics:
  - **Document management:** This topic specifies how to manage documents through the life cycle of creation, categorization, storage, retrieval, modification, and destruction. Topics covered include employee obligations, backup and archive, document retention policy, and enhanced protection for records
  - **Sensitive physical information:** The objective is to protect sensitive physical information in accordance with information security and regulatory requirements, preserve the integrity of sensitive physical information, and protect it from unauthorized disclosure. The SGP provides checklists for identification and labeling; storage of sensitive physical information; protection against unauthorized disclosure of sensitive physical information; secure transportation of sensitive physical information; and handling and disposing of sensitive physical information.

6.6 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

aggregation
appropriation
blackmail
breach of confidentiality
data loss prevention (DLP)
decisional interference
disclosure
distortion
document
document management
document management system
exclusion
exposure
General Data Protection Regulation (GDPR)
Identification
increased accessibility
information classification
information handling
information labeling
information type
insecurity
interrogation
intrusion
privacy
radio-frequency identification (RFID)

https://t.me/learningnets

records
records management
records management system
secondary use
security category
sensitive physical information
surveillance

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. The SGP divides information management into four topics. What are they?
2. Explain the NIST risk management framework's six-step approach to managing overall risk.
3. How does FIPS 199 define security categories?
4. Explain the four steps of the security categorization process included in NIST SP 800-60.
5. Name three sources suggested by SP 800-60 that define individual information types.
6. Explain the term *privacy* from an information point of view.
7. Does *privacy* have the same meaning as *information security*?
8. In today's information scenario, what are some possible types of threats in the information collection process?
9. How can privacy be violated at the information processing stage?
10. List some potential privacy threats that may occur as information is being disseminated.
11. What kind of privacy threats are exposed by invasions?
12. Enumerate and briefly explain key principles of the GDPR.
13. How does NIST SP 800-53 organize privacy controls?
14. Differentiate between the terms *document* and *record*.
15. What is the life cycle of a record?
16. What are some supporting technologies that can be used to protect sensitive physical information?
17. What are some key issues in securing physical information throughout its life cycle?

https://t.me/learningnets

6.7 References

CLAR14: Clark, D., Berson, T., & Lin, H. (Eds.), *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* National Research Council, 2014.

HEIS14: Higher Education Information Security Council, "Records Retention and Disposition Toolkit." *Information Security Guide*, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Records+Retention+and+Disposition+Toolkit.

JUDY14: Judy, H., et al., "Privacy in Cyberspace." In Bosworth, S., Kabay, M., & Whyne, E. (Eds.), *Computer Security Handbook.* Hoboken, NJ: Wiley, 2014.

KINA16: Kinast, K., *10 Key Facts Businesses Need to Note About the GDPR*. European Identity & Cloud Conference, 2016.

ROE10: Roe, D., "6 Ways Document Management and Records Management Differ." *CMS Wire*, January 25, 2010.

SOLO06: Solove, D., *A Taxonomy of Privacy.* GWU Law School Public Law Research Paper No. 129, 2006. http://scholarship.law.gwu.edu/faculty_publications/921/.

SPRA95: Sprague, R., "Electronic Document Management: Challenges and Opportunities for Information Systems Managers." *MIS Quarterly*, March 1995.

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Chapter 7

Physical Asset Management

"But I know nothing about hardware."

"Tut, my boy; you know about figures."

—*The Stock-Broker's Clerk*, Sir Arthur Conan Doyle

Learning Objectives

After studying this chapter, you should be able to:

- Describe the hardware life cycle management process.
- List and describe the threats to and vulnerabilities of office equipment.
- Discuss the security controls needed for office equipment.
- Understand the operational and security differences between IT systems and industrial control systems.
- Define the key elements in the ecosystem for mobile device use in an enterprise.
- Describe an effective mobile device security strategy.
- Present an overview of physical asset management best practices.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) uses the term **physical asset** to refer to all information and communications technology (ICT) hardware, including systems and network equipment; office equipment (such as, network printers and multifunction devices); mobile devices; and specialist equipment (for example, industrial control

https://t.me/learningnets

systems). The physical asset management category in the SGP comprises four topics, all of which are covered in this chapter:

- **Hardware life cycle management:** Deals with the management of the entire life cycle of hardware that is used to support enterprise information systems, including product selection, testing, deployment, and assessment.
- **Office equipment:** Covers peripheral devices such as printers, scanners, fax machines, and multifunction devices.
- **Industrial control systems:** Deals with security issues related to systems that monitor or control physical activities.
- **Mobile computing:** Deals with security issues related to the use of mobile devices in an enterprise information system.

7.1 Hardware Life Cycle Management

This section and the next two are concerned with protection of physical assets, including systems and network equipment, office equipment (for example, network printers, multifunction devices), and specialist equipment (for example, industrial control systems) throughout their life cycle, addressing the information security requirements for their acquisition (for example, purchase or lease), maintenance, and disposal. We begin with an examination of life cycle management issues for hardware in general and then look at specific issues related to office equipment and industrial control systems.

For purposes of this book, the definition of **hardware** from the SGP is used:

> **Hardware** is defined as any physical asset that is used to support corporate information or systems (e.g., a server, network device, mobile device, printer or specialized equipment, such as that used by manufacturing, transport or utility companies), including the software embedded within them and the operating systems supporting them.

Hardware life cycle management, also known as *hardware asset management* (*HAM*), is a subset discipline of IT asset management, which deals specifically with the hardware portion of IT assets. HAM entails managing the physical components of computers, computer networks and systems, beginning with acquisition and continuing through maintenance until the hardware's ultimate disposal.

https://t.me/learningnets

There are essentially two approaches to managing IT-related hardware assets within an organization. One is an ad hoc approach that follows guidance in the installation, configuration, and user's manual on a case-by-case basis with no overall approach. The other is an organized hardware life cycle management policy, perhaps under a designated hardware asset manager. There are a number of reasons an organization should adopt a detailed hardware life cycle management policy, including the following:

- While it is desirable to retain hardware for as long as reasonable to get the most use of an investment, it is important to avoid unnecessary costs, such as lowered productivity, increased downtime, and elevated levels of user dissatisfaction. A systematic approach to life cycle management can provide guidance on when to replace particular equipment.
- Organizations without the added discipline and visibility offered by HAM are often frustrated by the communication gaps that allow assets to be lost, acquisitions to be made when spares are in the warehouse, or upgrades to fail due to incomplete information.
- Hardware life cycles vary significantly from vendor to vendor. Accordingly, organizations should centralize hardware information in a **configuration management database (CMDB).**
- Various threats are associated with any type of hardware. An organization can reduce risk by having and using the appropriate tools to track and manage its hardware.
- There is a need to map hardware with the applications installed on that hardware for software compliance management and reporting. For example, if you have multiple desktop systems that have not been logged into in over six months and there is software installed on those systems, you should be able to, with the proper policies in place, remove that software and harvest, or recover, that software title for use somewhere else or retirement.
- With hardware life cycle management, an organization can use a number of automated tools for tasks such as inventory tracking and classification.

configuration management database (CMDB)

A repository containing information on all the devices, software, interconnections, and users in use, together with relevant configuration settings. Generally, a CMDB also includes historical configuration information.

Figure 7.1 illustrates the phases in hardware life cycle management. The first step is to plan for the management of hardware assets.

https://t.me/learningnets

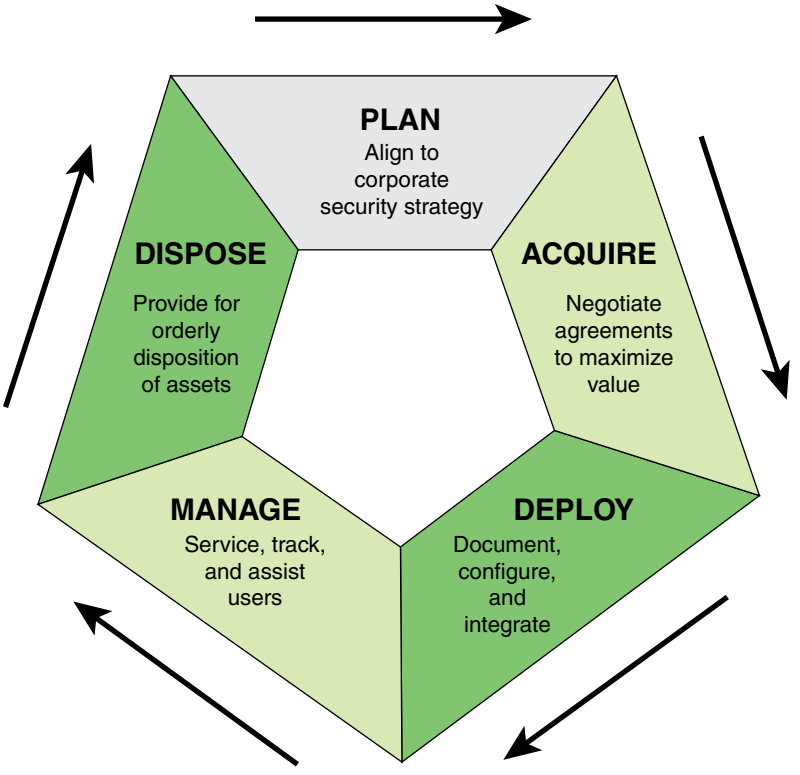


FIGURE 7.1 Hardware Asset Life Cycle

Planning

The results of the planning phase should include elements with which you are already familiar:

- **Strategic plan:** Includes designation of a responsible individual and a budget for HAM.
- **Security plan:** Relates to security controls in place for HAM and planned for meeting strategic security objectives.
- **Security policy:** Details how security concerns will be incorporated into the hardware life cycle.
- **Acceptable use policy:** Relates to how users are allowed to use hardware assets. In addition to security concerns, users need to be aware that the assets belong to the organization, without expectation of privacy, unless an organization's privacy policy dictates otherwise.

https://t.me/learningnets



International Association of Information Technology Asset Managers http://iaitam.org

The planning process should result in a definition of the mission, overall strategies, objectives, measurements, and prioritization for HAM actions in the organization. The plan should include guidelines for hardware selection, methods for identifying and controlling for security vulnerabilities, and a classification scheme.

As an aid to the planning process, the International Association of Information Technology Asset Managers offers advice and guidelines for acquiring, tracking, assessing, and disposing of hardware. In addition, there are companies that offer hardware life cycle management as an outsourced managed service.

Acquisition

A number of individuals and groups should be involved in the hardware acquisition process, including an acquisition manager, stakeholders, receivers, technical personnel, and the financial manager. The International Association of Information Technology Asset Managers [IAT12] states that the processes and systems of acquisition should include the following:

- **Request and approval:** Including application of standards, redeployment, and initiation of a purchase, if appropriate
- **Vendor relationships:** Including existing contracts and new opportunities
- **Acquisition:** With a formal selection processes, contract negotiations, and contracts execution
- **Receipt:** To trigger payment of invoices and creation of incidents to configure and deliver to the correct individual/location/department

The acquisition process should be designed to meet specific objectives, including:

- Gaining the most value from expenditures
- Strategic planning for system and application upgrades
- Reducing risk of data loss or breach
- Disposing of assets in a cost-effective manner that secures data and meets recycling goals

Deployment

Deployment refers to the preliminary steps taken prior to installation followed by the installation of the hardware so that it is ready to use. Each item should be categorized

https://t.me/learningnets

based on its security impact (for example, from very low to very high). The deployment process involves ensuring that any software running on the new hardware is subject to security hardening, such as changing default vendor passwords and applying secure configuration settings.

Automated asset identification, such as with a bar code or radio-frequency identification (RFID) tag, is often desirable. This supports inventory management, life cycle management, and, ultimately, disposal management.

Each hardware item needs to be included in a master register or database, perhaps as part of a CMDB. The register should be complete and protected.

Management

Once equipment is deployed, it needs to be maintained and managed in several ways. Preventive maintenance is high on the list of tasks to be performed. A manufacturer may recommend that an asset be serviced at certain times, but for some types of equipment and in some environments, the manner in which the asset is actually used day-to-day may require that it be serviced on a faster or slower schedule. For example, sensor equipment in a factory environment may be exposed to harsh environmental conditions, necessitating frequent preventive maintenance.

For larger companies, tracking of hardware assets is a key task. Larger organizations often have an entire department devoted to IT tracking. Asset location technologies, such as RFID, can help organizations ensure that critical assets, such as essential information system components, remain in authorized locations. Such capability may also help organizations rapidly identify the location of and individuals responsible for system components that have been compromised, breached, or are otherwise in need of mitigation actions. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, in control family CM-1, provides detailed guidance in the area of tracking and IT hardware configuration management.

Acquisition processes require ongoing management supported through policies and backed by measurements. Measurement requires data and the ability to interpret beyond the silos of individual process steps. Examples of measurements include customer satisfaction, the vendor's compliance with the contract, usage, and strategic impact.

Hardware should be serviced/maintained on a regular basis. The simplest approach is to schedule maintenance in accordance with supplier/manufacturer recommendations. Particularly in larger organizations, it may be cost-effective to attempt to optimize the

https://t.me/learningnets

maintenance program. As an example, IBM offers a solution called Predictive Maintenance and Quality (PMQ) that uses information collected about products, processes, and assets to optimize maintenance schedules, production processes, and product quality [IBM14]. This integrated solution brings a variety of benefits to an enterprise, including the following:

- Predicting the best time to perform maintenance on a monitored asset
- Uncovering process deficiencies that can affect product quality
- Identifying the root causes of asset failures

Disposition

An important part of the IT hardware life cycle is disposition, which may be destruction, recycling, or redeployment. Examples of savings from redeployment include:

- Continuing to use leased hardware assets prior to lease termination
- Eliminating the purchase of new hardware
- Speeding delivery to the end user as redeployment is generally faster than deployment involving ordering and receiving new assets

When hardware items are to be destroyed, it is important to securely destroy all information stored on the hardware.

Whatever the type of disposition, life cycle management should include planning for the likely dates when disposition decisions need to be made on various equipment. Table 7.1 lists typical values for the useful lifetimes of various types of hardware [GARR10].

TABLE 7.1 The Average Life Cycle Duration of Common Hardware

Hardware	Duration
Cell phones	2 years
Laptop PC	3 years
Desktop PC	4 years
Server	5 years
Networking gear	5 years
Monitor	8 years

https://t.me/learningnets

7.2 Office Equipment

The SGP defines **office equipment** as follows:

> **Office equipment** includes printers, photocopiers, facsimile machines, scanners, and multifunction devices (MFDs). Office equipment often contains the same components as a server (e.g., operating system, hard disk drives, and network interface cards) and runs services such as web, mail, and ftp. As a result, sensitive information processed by or stored on office equipment is subject to similar threats as to servers, yet this equipment is often poorly protected.

A *multifunction device* (*MFD*) is generally defined as a network-attached document production device that combines two or more of these functions: copy, print, scan, and fax.

Most office equipment devices contain some processing power and storage capability, and in the office setting, such devices are frequently attached to a network. Thus, most such devices are both assets to protect and opportunities for threat. Such equipment often is not provided with the necessary security controls to meet risk management objectives.

Threats and Vulnerabilities

There are numerous potential threats to office equipment. The following sections look at a number of threats, based on the SANS Institute article "Auditing and Securing Multifunction Devices" [SCOT07] and NISTIR 8023, *Risk Management for Replication Devices*.

Network Services

MFDs often come with a number of services enabled, many of which are not required in a given environment and should be disabled. Two categories of network services are:

- **Management protocols:** These protocols, which are provided to enable a device to be configured and managed over a network, include Hypertext Transfer Protocol (HTTP) and HTTP over SSL or HTTP Secure (HTTP/HTTPS) (web interface), Telnet (text-based interface), and Simple Network Management Protocol (SNMP) (monitoring and configuration protocol). With these protocols, an attacker may be able to access and possibly modify configuration information and to gather authentication information.
- **Services protocols:** These protocols enable the user to send and receive data from a printer, fax, copier, or MFD. They protocols, including HP JetDirect, Line Printer Daemon, Internet Printing Protocol, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP), generally send data in the clear

https://t.me/learningnets

and have limited security features. Threats include unauthorized remote printing and observing jobs sent in plaintext. In addition, FTP allows TCP port 9100 service, over which most printing takes place and which is often used as a control port. Threats include unauthorized remote printing and capture of spool files. An MFD may also be vulnerable to an FTP bounce attack, in which the attacker uses a proxy feature that allows a user to request that one FTP server copy files to another. Most FTP servers do not allow this feature, but it is still possible on a number of them. It can be used to bypass firewall protection. SMTP may be used to support an inbound SMTP-to-fax service and outbound SMTP to send scanned documents to owners. SMTP transfers are unencrypted, creating vulnerability. Also, an inbound SMTP server might be used as an SMTP relay, allowing for spamming.

Information Disclosure

The vulnerabilities just discussed may expose user data and configuration information. In addition, the SANS Institute [SCOT07] points out that read-only access to an MFD's web-based management interface or SNMP information is sometimes all that is needed for a social engineer to gather valuable information about an organization and its business practices. Three potential sources of vulnerability are:

- **Print, fax, and copy/scan logs:** Print logs present the threat of exposure of sensitive document names, network usernames, and URLs of websites users have printed from. Fax numbers indicate with whom an organization does business, and long-distance codes/long-distance credit card numbers may show up with dialed numbers. Copy/scan logs can expose email addresses of recipients and logon information for FTP file uploads.
- **Address books:** Some MFDs allow the user to create address books as distribution or destination lists. This may expose internal and customer email addresses and fax numbers, long-distance codes and credit card numbers, and server addresses and usernames for FTP sites.
- **Mailboxes:** MFDs may contain mailboxes used to store scans, faxes, or templates. Unless it is password protected, a mailbox could provide an attacker with entire faxes or scanned documents containing sensitive information.

denial-of-service (DoS) attack
An attack that prevents authorized access to resources or delays time-critical operations

Denial-of-Service Attacks

MFDs can be vulnerable to a number of **denial-of-service (DoS) attacks**. According to Crenshaw's article "Hacking Network Printers" [CREN17], these include sending multiple bogus print jobs to exhaust paper resources and tie up a printer, modifying settings to make the device unusable, stopping or deleting jobs, and setting the IP address of the MFD to be the same as a router, causing routing confusion.

https://t.me/learningnets

NISTIR 8023 points out that most devices, if not properly configured, process any submitted job, without regard to the originator, without confirmation that the job is authorized, and without authentication. If exploited, this vulnerability may waste ink, paper, toner, or other materials while also resulting in denial of service for legitimate users.

Physical Security

Proper physical security is needed to guard against a number of threats, including the following:

- Making modifications to the global configuration via the console interface. While this can happen maliciously, it can also happen unintentionally when a user, an IT staff person, or a vendor troubleshoots the device. Someone might set a device back to factory defaults to clear up a problem and then only enter the bare minimum configuration, thus erasing any security hardening you may have done.
- Sending unauthorized faxes.
- Obtaining printouts or faxes that do not belong to them.
- Physically removing the hard disk, which might contain print spool files and other information.

This last threat relates to what to do when it is time to dispose of a device, discussed subsequently in this section.

Operating System Security

Another general area of vulnerability cited by NISTIR 8023 is the operating system of the MFD. Many office devices run an embedded commercial operating system, which renders them subject to the same threats and vulnerabilities as any other computing devices running those same operating systems. To complicate matters, manufacturers may embed versions of operating systems for which the operating system provider is no longer providing updates or the functionality to install patches or updates is not available. Buffer overflows, execution of arbitrary code, and taking control of the device using remote administration capabilities via web server or website are but a few examples of exploits to which remote devices (RDs) with unpatched operating systems and firmware are vulnerable.

Security Controls

A useful checklist of security measures an organization can take to protect MFDs is provided in the SANS Institute article "Auditing and Securing Multifunction Devices" [SCOT07] and shown in Table 7.2.

https://t.me/learningnets

TABLE 7.2 Multifunction Device Hardening Checklist

Category	Action
Network protocols and services	Disable unused network protocols other than TCP/IP. Disable unused network services (print/fax/scan and management). Assign the MFD a static IP address. Restrict access to MFD services (print/fax/scan and management) to the minimum number of hosts that require these functions. Use encrypted communications protocols (for example, HTTPS), where available, and disable insecure protocols.
Management	Set a strong administrator password. Change default SNMP community strings to strong passwords. Use SNMP encryption, if supported. Ensure that logging is enabled on the MFD. Ensure that logs are monitored on a regular basis. Restrict access to address books, mailboxes, and logs using your current password policy.
Security updates	Monitor CVEs and vendor for security bulletins and patches. Upgrade firmware in a timely manner, using your current change control process.
Physical security	Place the device in an area with physical security controls consistent with the sensitivity of the data it processes. Set an administrator password on the console. Require that users authenticate to scan, fax, or copy from the console. If the MFD has a removable hard drive, ensure that it is locked into the device. If possible, implement measures to encrypt or securely wipe print spool files. Ensure that your security policy specifies what to do with MFD drives that are decommissioned or sent back to the manufacturer or leasing company (for example, retained, securely wiped, destroyed).

A more comprehensive list is provided by the Center for Internet Security (CIS) [CIS09], which defines a set of benchmark recommendations using two configuration levels:

- **Level 1:** Intended to be practical and prudent, provide a clear security benefit, and not negatively inhibit the utility of the technology
- **Level 2:** Intended to provide a higher level of defense but may negatively inhibit the utility or performance of the technology

https://t.me/learningnets

The choice of measures should depend on the organization's risk assessment relative to a particular office device asset. The CIS describes a total of 39 level 1 benchmarks and 2 level 2 benchmarks in the following areas:

- **Physical device management:** The benchmarks cover three categories:
  - **Physical connections:** Measures include disabling 1394 and serial connectors, limiting physical access to authorized users, requiring a PIN or other access code, and verifying configuration state after a power loss.
  - **Hard drive and memory:** Measures include configuring for encryption of data at rest (if available), using physical locks, deleting completed scan jobs, and erasing the hard drive before disposal.
  - **Firmware:** Measures include establishing a procedure to ensure that the current version of the firmware is used.
- **Remote device management:** The benchmarks cover three categories:
  - **TCP/IP configuration:** Measures include using a static IP address, disabling various ports and protocols, and limiting network accessibility to ingress from authorized subnets and ports.
  - **Wireless access configuration:** Measures include disabling unused Bluetooth and Wi-Fi interfaces.
  - **Use of secure management protocols:** Measures include disabling a number of insecure access methods, such as FTP, and relying on secure SNMPv3.
- **Job access and processing:** This area includes requiring a PIN for confidential job retrieval and accepting jobs from only authorized spoolers and users.
- **Application development platforms:** The benchmarks cover two categories:
  - **Application signatures:** Measures include requiring valid and trusted digital signature for all applications and requiring that an application signature be provided by a trusted authority.
  - **Package management:** Measures include uninstalling or disabling all unused software-based packages .
- **User management:** MFDs are typically preconfigured with default user accounts. The organization should change the default usernames and passwords.

https://t.me/learningnets

- **Logging and monitoring:** Office devices commonly contain functionality to log activities, such as print spooler access, print jobs, print to fax, email, and file sharing. The organization should enable all logging activity.
- **Miscellaneous:** The CIS addresses secure configuration of two additional capabilities: replacing self-signed certificates with trusted certificates and restricting access to scans placed on a remote file share.

For each of the benchmarks, CIS provides a description of the benchmark and a rationale for its implementation.

Equipment Disposal

self-encrypting drive (SED)
A hard drive with a circuit built into the disk drive controller chip that encrypts all data to the magnetic media and decrypts all the data from the media automatically. All SEDs encrypt all the time from the factory onward, performing like any other hard drive, with the encryption being completely transparent or invisible to the user. To protect the data from theft, the user must provide a password to read from or write data to the disk.

cryptographic erasure
The process of encrypting the data on a medium and then destroying the key, making recovery impossible.

The SGP recommends that sensitive information stored on office equipment be securely destroyed (for example, by using deletion software or physically destroying the hard disk drives) before the equipment is decommissioned, sold, or transferred to an external party (for example, a leasing company or equivalent). This is an important security area that should not be overlooked as part of an organization's security program for office devices.

An excellent source of guidance in this area is NIST SP 800-88, *Guidelines for Media Sanitization*. The document defines *media sanitization* as a process of rendering access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. Three increasingly secure actions for sanitization are defined:

- **Clear:** Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge:** Applies physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques. This can be achieved by performing multiple overwrites. For a **self-encrypting drive (SED)**, **cryptographic erasure** can be used. If the drive automatically encrypts all user-addressable locations, then all that is required is to destroy the encryption key, which could be done by multiple overwrites.
- **Destroy:** Renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. Typically, the medium is pulverized or incinerated at an outsourced metal destruction or licensed incineration facility.

https://t.me/learningnets

Based on the risk assessment for an office device, an organization can assign a security category to the data on the device and then use the flowchart of Figure 7.2 to determine how to dispose of the memory associated with the device.

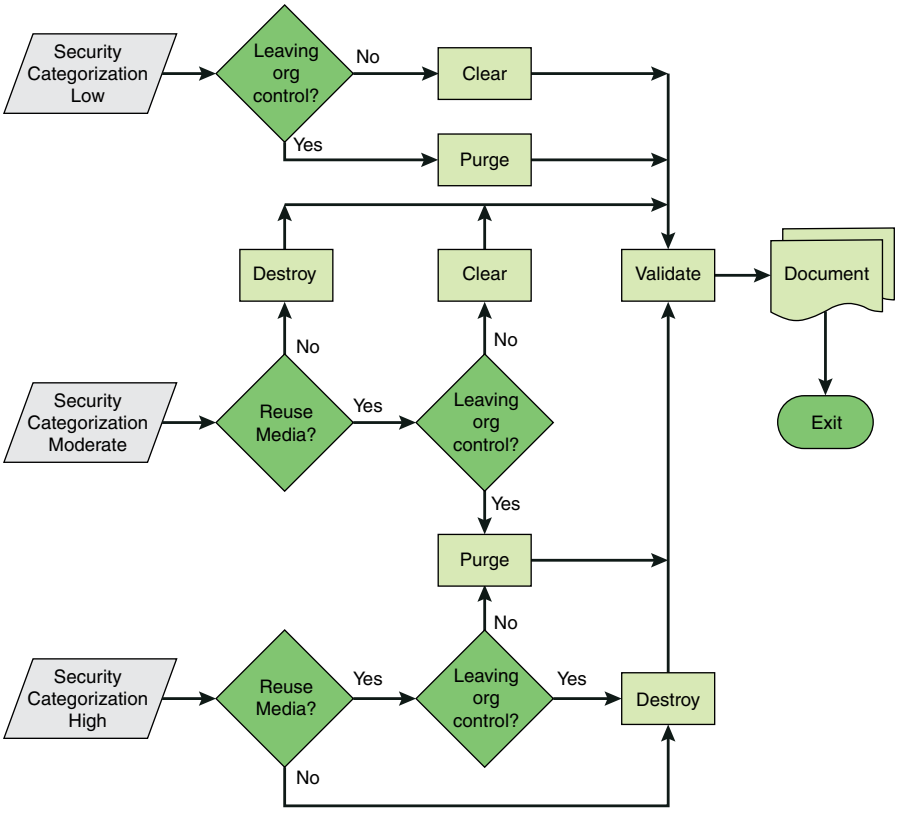


FIGURE 7.2 Sanitization and Disposition Decision Flow

7.3 Industrial Control Systems

An industrial control system (ICS) is used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems, using programmable logic controllers to control localized processes. An ICS consists of combinations of control components (for example, electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (for example, manufacturing, transportation of matter or energy).

https://t.me/learningnets

Figure 7.3, based on a figure in SP 800-82, *Guide to Industrial Control Systems Security*, illustrates the principal elements of an industrial control system and their operational interaction.

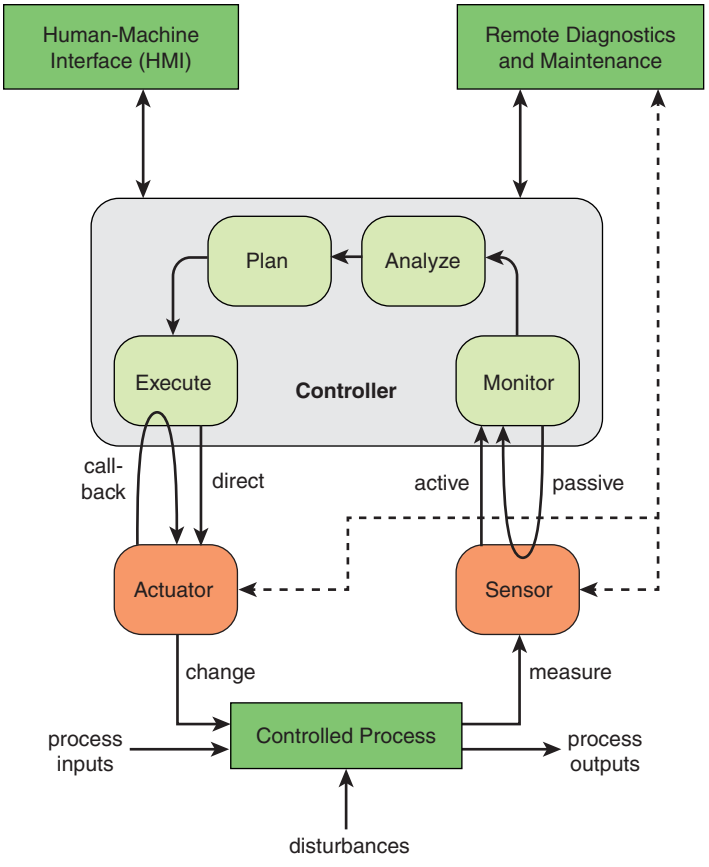


FIGURE 7.3 ICS Operation

The elements of an ICS are as follows:

- **Sensor:** A sensor measures some parameter of a physical, chemical, or biological entity and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal. In both cases, the sensor output is typically input to a microcontroller or other management element.
- **Actuator:** An actuator receives an electronic signal from a controller and responds by interacting with its environment to produce an effect on some parameter of a physical, chemical, or biological entity.

https://t.me/learningnets

- **Controller:** The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. The controller may have very limited intelligence and may rely on the human–machine interface for direction. But typically, a controller adjusts the directives given to actuators automatically, based on sensor input.
- **Human–machine interface:** Operators and engineers use human interfaces to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The human interface also displays process status information and historical information.
- **Remote diagnostics and maintenance:** Diagnostics and maintenance utilities are used to prevent, identify, and recover from abnormal operation or failures.

Differences Between IT Systems and Industrial Control Systems

Industrial control systems and IT systems differ in a number of ways. Most obviously, ICSs control elements in the physical world, and IT systems manage data. While both must deal with security threats, the nature of the risks differs. Table 7.3, based on SP 800-82, lists key differences between IT systems and ICSs.

TABLE 7.3 Differences Between IT and Industrial Control Systems

Category	IT Systems	ICSs
Performance requirements	Operation is non-real-time. Response must be consistent. High throughput is demanded. High delay and jitter may be acceptable. Response to human and other emergency interaction is generally not critical. Tightly restricted access control can be implemented to the degree necessary for security.	Operation is real-time. Response is time-critical. Modest throughput is acceptable. High delay and/or jitter is not acceptable. Response to human and other emergency interaction is critical. Access to ICS should be strictly controlled but should not hamper or interfere with human–machine interaction.

https://t.me/learningnets

Category	IT Systems	ICSs
Availability (reliability) requirements	Responses such as rebooting are acceptable. Availability deficiencies can often be tolerated, depending on the system's operational requirements.	Responses such as rebooting may not be acceptable because of process availability requirements. Availability requirements may necessitate redundant systems. Outages must be planned and scheduled days or weeks in advance. High availability requires exhaustive pre-deployment testing.
Risk management requirements	Manage data. Data confidentiality and integrity are paramount. Fault tolerance is less important; momentary downtime is not a major risk. The major risk impact is delay of business operations.	Control physical world. Human safety is paramount, followed by protection of the process. Fault tolerance is essential; even momentary downtime may not be acceptable. Major risk impacts are regulatory noncompliance, environmental impacts, and loss of life, equipment, or production.
System operation	Systems are designed for use with typical operating systems. Upgrades are straightforward, using automated deployment tools.	Systems include differing and possibly proprietary operating systems, often without built-in security capabilities. Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved.
Resource constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions.	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities.
Communications	Standard communications protocols are used. Primarily wired networks are used, with some localized wireless capabilities. Typical IT networking practices are used.	Many proprietary and standard communication protocols are used. Several types of communications media are used, including dedicated wire and wireless (radio and satellite). Networks are complex and sometimes require the expertise of control engineers.

https://t.me/learningnets

Category	IT Systems	ICSs
Change management	Software changes are applied in a timely fashion in the presence of good security policies and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICSs may use operating systems that are no longer supported.
Managed support	Diversified support styles are possible.	Service support is usually via a single vendor.
Component lifetime	Component lifetime is on the order of 3 to 5 years.	Component lifetime is on the order of 10 to 15 years.
Components location	Components are usually local and easy to access.	Components can be isolated or remote and may require extensive physical effort to gain access to them.

ICS Security

Just as there are differences in the operation and environment between ICSs and IT systems, there are also differences in security risks and countermeasures. An ICS often involves widely distributed devices that may be in insecure locations. In many cases, these are embedded devices containing microcontrollers with limited processing power and limited human interface functionality. Table 7.4, based on the Department of Homeland Security's (DHS's) *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* [DHS16], compares the security functions for ICS and IT systems.

TABLE 7.4 Security Functions for IT Systems and Industrial Control Systems

Security Area	IT Systems	ICSs
Antivirus and mobile code	Very common Easily deployed and updated User control over customization, which can be asset based or enterprise based	Memory requirements Ability to protect legacy systems with after-market solutions "Exclusion" folders required to avoid programs quarantining critical files
Patch management	Easily defined Enterprisewide Remote and automated	Long timeline to successful patch installation OEM specific May "break" ICS functionality Asset owners required to define acceptable risk

https://t.me/learningnets

Security Area	IT Systems	ICSs
Technology support lifetime	2–3 years Multiple vendors Ubiquitous upgrades	10–20 years Usually the same vendor over time New security concerns at product end-of-life
Testing and audit methods	Modern methods Systems usually resilient and robust to handle assessment methods	Tune testing to the system Modern methods possibly inappropriate Equipment possibly susceptible to failure during testing
Change management	Regular and scheduled Aligned with minimum-use periods	Strategic scheduling Non-trivial process due to impact on production
Asset classification	Common and performed annually Results drive expenditure	Performed only when obligated Accurate inventories uncommon for nonvital assets Disconnect between asset value and appropriate countermeasures
Incident response and forensics	Easily developed and deployed Some regulatory requirements Embedded in technology	Focused on system resumption activities Forensics procedures immature (beyond event re-creation) Requires good IT system/ICS relationships
Physical and environmental security	Can range from poor (office systems) to excellent (critical IT operations systems)	Usually excellent for critical areas Maturity varies for site facilities based on criticality/culture
Secure systems development	Integral part of the development process	Historically not an integral part of the development process Vendors maturing but at slower rate than IT Core/flagship ICS solutions difficult to retrofit with security
Security compliance	Definitive regulatory oversight, depending on the sector (and not all sectors)	Specific regulatory guidance, depending on the sector (and not all sectors)

The Patching Vulnerability

In an often-quoted 2014 article, security expert Bruce Schneier stated that we are at a crisis point with regard to the security of embedded systems, including Internet of Things (IoT) devices and ICSs [SCHN14]. Embedded devices are riddled with vulnerabilities, and there is no good way to patch them. Chip manufacturers have

https://t.me/learningnets

strong incentives to produce their products, with firmware and software, as quickly and inexpensively as possible. Device manufacturers choose chips based on price and features and do very little, if anything, to chip software and firmware. Their focus is the functionality of the device itself. The end user may have no means of patching the system or little information about when and how to patch. The result is that the hundreds of millions of Internet-connected devices in the IoT are vulnerable to attack. This is certainly a problem with sensors, allowing attackers to insert false data into networks. It is potentially a graver threat with actuators, with which attacker may be able to affect the operation of machinery and other devices.

Typical Security Threats to ICSs

As mentioned earlier, a number of threats are specific to ICSs. According to SP 800-82, possible threats ICSs may face include the following:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life.

Key Security Measures

The DHS has offered these recommendations for protecting ICSs [DHS15]:

- **Implement application whitelisting:** This is the practice of specifying an index/list of approved software applications that are permitted to be present and active on a computer system and preventing execution of all other software on the system. The goal of whitelisting is to protect computers and networks from potentially harmful applications and malware.

https://t.me/learningnets

- **Ensure configuration management and patch management:** A major source of vulnerabilities with ICS devices is software and hardware flaws that can be targeted by adversaries. Configuration management is the process of controlling modifications to a system's hardware, software, and documentation, which provides sufficient assurance that the system is protected against the introduction of improper modification before, during, and after system implementation. Patch management is the systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. Patch management tasks include maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required.
- **Reduce attack surface areas:** Techniques for reducing the **attack surface** include isolating ICS networks from any untrusted networks, especially the Internet, locking down all unused ports, turning off all unused services, and allowing real-time connectivity to external networks only if there is a defined business requirement or control function.
- **Build a defendable environment:** The objective is to limit damage from network perimeter breaches. A common approach is to segment networks into logical enclaves and restrict host-to-host communications paths. This can stop adversaries from expanding their access, while allowing the normal system communications to continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves.
- **Manage authentication:** Adversaries are increasingly focusing on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Compromising these credentials allows adversaries to masquerade as legitimate users, leaving less evidence than when exploiting vulnerabilities or executing malware. Recommended countermeasures include requiring **multifactor authentication (MFA)** and enforcing the principle of **least privilege** (POLP).
- **Implement secure remote access:** Some adversaries are effective at gaining remote access into control systems, finding obscure access vectors, and even finding "hidden back doors" intentionally created by system operators. System managers should remove such accesses wherever possible and require remote access to be operator controlled and time limited.

attack surface
The reachable and exploitable vulnerabilities in a system.

multifactor authentication (MFA)
The use of two or more factors to achieve authentication. Factors include something you know (for example, password/PIN), something you have (for example, cryptographic identification device, token), or something you are (for example, biometric). MFA can involve two or three factors.

least privilege
The principle that access control should be implemented so that each system entity is granted the minimum system resources and authorizations needed for the entity to do its work. This principle tends to limit damage that can be caused by an accident, an error, or a fraudulent or unauthorized act.

https://t.me/learningnets

- **Monitor and respond:** Defending a network against modern threats requires active monitoring for adversarial penetration and quick execution of a prepared response. The monitoring function should include analyzing access logs and verifying all anomalies. The response plan may include disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100% password reset. It is important to ensure that the restore includes **golden records** that restore systems to last known good state.

golden record
A collection of data records, in a centralized database or a synchronized distributed database, defined to be authoritative within the organization. The golden record encompasses all relevant data entities in the organizational information system. The golden record can be used as a basis for reconciliation, as a guarantee of data integrity, and as the basis for backups and archives. Also called **single version of truth**.

Resources for ICS Security

The best resource in developing a security plan for an ICS is the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) website, maintained by the U.S. Department of Homeland Security. The site contains a wide range of advisories, fact sheets, and white papers and is frequently updated.

Several publications available at this site are particularly useful:

- ***Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*** **[DHS16]:** Discusses ICS attack methods, a set of defense-in-depth strategies, and specific recommendations for securing and ICS.
- ***Cyber Security Assessments of Industrial Control Systems*** **[DHS10]:** Describes in detail methods for assessing the security policies and controls for an ICS.
- **SP 800-82,** ***Guide to Industrial Control Systems Security*****:** Provides an overview of ICSs; ICS risk management; security program development and deployment; a recommended ICS security architecture; risk management for an ICS; and guidance on applying the SP 800-53 security controls for an ICS.
- ***Catalog of Control Systems Security: Recommendations for Standards Developers*** **[DHS11]:** Provides detailed descriptions of 250 recommended security controls in 19 categories.



Industrial Control Systems Cyber Emergency Response Team https://ics-cert.us-cert.gov

7.4 Mobile Device Security

This section discusses security issues relevant to the use of mobile devices within an organization or to access organization assets from remote locations. SP 800-53 defines a **mobile device** as a "portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices)."

https://t.me/learningnets

Prior to the widespread use of smartphones, there was a dominant paradigm for computer and network security. Corporate IT was tightly controlled. User devices were typically limited to Windows PCs. Business applications were controlled by IT and either run locally on endpoints or on physical servers in data centers. Network security was based on clearly defined perimeters that separated trusted internal networks from the untrusted Internet. Today, there have been massive changes in these assumptions. An organization's networks must accommodate the following:

- **Growing use of new devices:** Organizations are experiencing significant growth in employee use of mobile devices. In many cases, employees are allowed to use a combination of endpoint devices as part of their day-to-day activities.
- **Cloud-based applications:** Applications no longer run solely on physical servers in corporate data centers. Today applications can run anywhere—on traditional physical servers, on mobile virtual servers, or in the cloud. In addition, end users can now take advantage of a wide variety of cloud-based applications and IT services for personal and professional use. Facebook can be used for an employee's personal profiles or as a component of a corporate marketing campaign. Employees depend on Skype to speak with friends abroad and for business video conferencing. Services such as Dropbox and Box can be used to distribute documents between corporate and personal devices for mobility and user productivity.
- **De-perimeterization:** Given the proliferation of new devices, application mobility, and cloud-based consumer and corporate services, the notion of a static network perimeter is all but gone. Now there are a multitude of network perimeters around devices, applications, users, and data. These perimeters have also become quite dynamic as they must adapt to various environmental conditions, such as user roles, device types, server virtualization mobility, network locations, and time of day.
- **External business requirements:** An enterprise must also provide guests, third-party contractors, and business partners network access using various devices from a multitude of locations.

The central element in all these changes is the mobile computing device. Mobile devices have become an essential element for organizations as part of the overall network infrastructure. Mobile devices such as smartphones, tablets, and memory sticks provide increased convenience for individuals as well as the potential for increased productivity in the workplace. Because of the widespread use and unique

https://t.me/learningnets

characteristics of mobile devices, security for these devices is a pressing and complex issue. In essence, an organization needs to implement a security policy through a combination of security features built into the mobile devices and additional security controls provided by network components that regulate the use of the mobile devices.

We can define a mobile Internet device as any portable technology running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple's iOS, Windows Mobile, and Symbian. The definition excludes technology running traditional/classic or more general-purpose operating systems, such as any of the Microsoft Windows desktop or server operating systems, versions of MacOS, or Linux.

Mobile Device Technology

Providing enterprise security for mobile devices is extraordinarily complex, both because of the technology of these devices and the ecosystem in which they operate. First, let's consider the technology involved in mobile devices. NISTIR 8023, *Risk Management for Replication Devices*, defines four layers in the mobile device technology stack (see Figure 7.4):

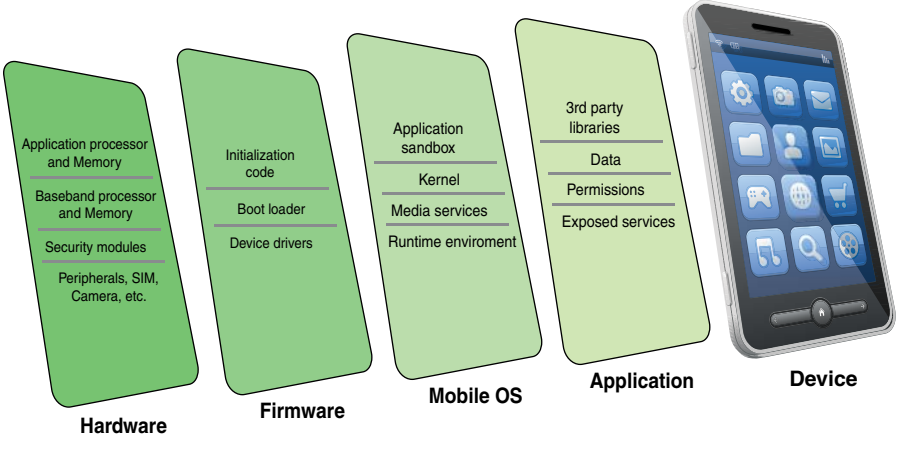


FIGURE 7.4 Mobile Device Technology Stack

- **Hardware:** The base layer of the technology stack is the device hardware. This includes an application processor, with the ARM family of processors being the most common. There is also a separate processor that runs the cellular network processor, typically referred to as the *baseband processor*. In addition,

https://t.me/learningnets

there may be hardware encryption modules and other security modules. The hardware layer also includes the peripherals incorporated into the device, such as the camera and SIM card. Vulnerabilities at this level can serve as attack vectors. Because the software of these components is embedded in the chips themselves, such vulnerabilities can be difficult to remediate.

- **Firmware:** The firmware necessary to boot the mobile operating system (that is, bootloader) may verify additional device initialization code, device drivers used for peripherals, and portions of the mobile operating system—all before a user can use the device. If the initialization code is modified or tampered with in some manner, the device may not properly function, or an attacker may be able to tamper with the operating system code and load an alternate version with malicious behavior.
- **Mobile operating system:** The most common operating systems for mobile devices are Android and iOS. An operating system includes a sandbox facility for isolating third-party applications in some manner to prevent unexpected or unwanted interaction between the system, its applications, and applications' respective data (including user data). The operating system layer also includes a runtime environment for applications and common services for multimedia. As with any other operating system, vulnerabilities are routinely discovered in mobile device operating systems. However, the development of patches and the update of the software are outside the control of the enterprise and in the hands of the operating system provider. In many instances, there have been long periods in which operating system vulnerabilities have been left unpatched due to the complex patch management life cycle of the operating system provider [DHS17].
- **Application:** The application layer includes third-party applications, various apps and services provided by the mobile device vendor, and facilities for defining permissions.

Mobile Ecosystem

The execution of mobile applications on a mobile device may involve communication across a number of networks and interaction with a number of systems owned and operated by a variety of parties. This ecosystem makes the achievement of effective security challenging.

Figure 7.5, based on one in NISTIR 8144, illustrates the main elements in the ecosystem within which mobile device applications function:

https://t.me/learningnets

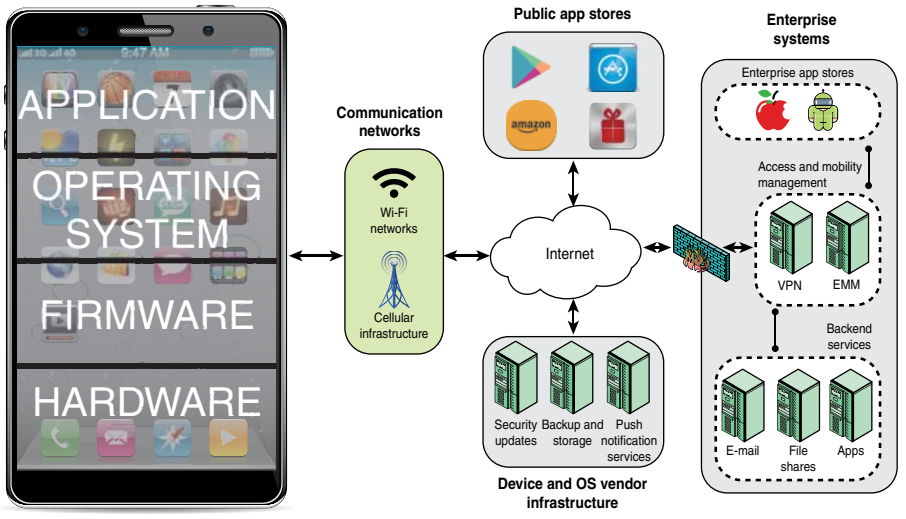


FIGURE 7.5 Mobile Ecosystem

- **Cellular and Wi-Fi infrastructure:** Modern mobile devices are typically equipped with the capability to use cellular and Wi-Fi networks to access the Internet and to place telephone calls. Cellular network cores also rely on authentication servers to use and store customer authentication information.
- **Public application stores (public app store):** Public app stores include native app stores, which are digital distribution services operated and developed by mobile operating system vendors. For Android, the official app store is Google Play, and for iOS, it is simply called the App Store. These stores invest considerable effort in detecting and thwarting malware and assuring that the apps do not cause unwanted behavior on the mobile device. In addition, there are numerous third-party app stores. The danger with third-party stores is that their apps may not be guaranteed to be free of malware.
- **Private application stores (private app store):** Many enterprises maintain their own app stores that offer applications of specific utility to the enterprise, either for Android, iOS, or both.
- **Device and OS vendor infrastructure:** Mobile device and operating system vendors host servers to provide updates and patches to operating systems and apps. Other cloud-based services may be offered, such as storing user data and wiping missing devices.

https://t.me/learningnets

- **Enterprise mobility management systems:** *Enterprise mobility management* (*EMM*) is a general term that refers to everything involved in managing mobile devices and related components (such as wireless networks). EMM is much broader than just information security; it includes mobile application management, inventory management, and cost management. Although EMM systems are not directly classified as a security technology, they can help in deploying policies to an enterprise's device pool and monitoring device state.
- **Enterprise mobile services:** These back-end services are accessible from authorized users' mobile devices, including email, file sharing, and other applications.

app store
An online repository of applications that can be browsed, purchased, and downloaded.

Vulnerabilities

Mobile devices need additional specialized protection measures beyond those implemented for other client devices, such as desktop and laptop devices that are used only within the organization's facilities and on the organization's networks. SP 800-124, *Guidelines for Managing and Securing Mobile Devices in the Enterprise*, lists seven major security concerns for mobile devices, examined in the following sections.

Lack of Physical Security Controls

Mobile devices are typically under the complete control of the user and are used and kept in a variety of locations outside the organization's control, including off premises. Even if a device is required to remain on premises, the user may move the device within the organization between secure and insecure locations. Thus, theft and tampering are realistic threats.

The security policy for mobile devices must be based on the assumption that any mobile device may be stolen or at least accessed by a malicious party. The threat is twofold: A malicious party may attempt to recover sensitive data from the device itself or may use the device to gain access to the organization's resources.

Use of Untrusted Mobile Devices

In addition to company-issued and company-controlled mobile devices, virtually all employees have personal smartphones and/or tablets. An organization must assume that these devices are not trustworthy. That is, the devices may not employ encryption, and either the user or a third party may have installed a bypass to the built-in restrictions on security, operating system use, and so on.

https://t.me/learningnets

Use of Untrusted Networks

If a mobile device is used on premises, it can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from the Internet to the organization. Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks. Thus, a security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy.

Use of Applications Created by Unknown Parties

By design, it is easy to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software. An organization has several options for dealing with this threat, as described later in this chapter.

Interaction with Other Systems

A common feature on smartphones and tablets is the ability to automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage. Unless an organization has control of all the devices involved in synchronization, there is a considerable risk that the organization's data will be stored in an unsecured location, and there is also a risk of malware introduction.

Use of Untrusted Content

Mobile devices may access and use content that other computing devices do not encounter. An example is the quick response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. A QR code translates to a URL, and a malicious QR code could direct mobile devices to malicious websites.

Use of Location Services

The GPS capability on mobile devices can be used to maintain knowledge of the physical location of the device. While this feature might be useful to an organization as part of a presence service, it creates security risks. An attacker can use the location information to determine where the device and user are located, which may be helpful to the attacker.

https://t.me/learningnets

Mobile Device Security Strategy

The recent DHS report *Study on Mobile Device Security* [DNS17] groups security threats and defenses into five primary components of the mobile ecosystem and their associated attack surface: the mobile device technology stack, mobile applications, mobile network protocols and services, physical access to the device, and enterprise mobile infrastructure (see Table 7.5). This is a useful way of organizing the security strategy for mobile devices. The following sections examine these five primary components in more detail.

rooting

The act of removing a restricted mode of operation. For example, rooting may enable content with digital rights to be used on any computer, or it may allow enhanced third-party operating systems or applications to be used on a mobile device. While rooting is the term used for Android devices, **jailbreaking** is the equivalent term used for Apple's devices.

sideloading

The act of downloading an app to a device without going through the official app store, via links or websites. While enterprises often use sideloading as a method for distributing homegrown apps, malicious actors also use sideloading (via enterprise certificates in many cases bought on the black market) to distribute their malware.

TABLE 7.5 Common Mobile Device Threats

Mobile Ecosystem Element	Threats
Mobile device technology stack	Delays in security updates Zero-day exploits against software and firmware, particularly the baseband Bootloader exploitation **Jailbreaking/rooting** **Sideloading** Supply chain compromise Trusted Execution Environment (Android) or Secure Enclave (iOS) exploitation Compromised cloud system credentials
Mobile applications	Malware (including backdoors, ransomware, and privilege escalation) Vulnerable third-party libraries Exploitation of vulnerable apps Insecure app development practices Exploitation of a public mobile app store
Mobile networks	Rogue cellular base stations and Wi-Fi access points Man-in-the-middle attacks on communications Data/voice eavesdropping Data/voice manipulation Device and identity tracking DoS/jamming

https://t.me/learningnets

Mobile Ecosystem Element	Threats
Device physical systems	Loss or theft of a mobile device Physical tampering Malicious charging station
Mobile enterprise	Compromised EMM/MDM system or admin credentials Compromised enterprise mobile app store or developer credentials Bypassed app vetting

Mobile Device Technology Stack

A number of organizations supply mobile devices for employee use and preconfigure those devices to conform to the enterprise security policy. However, many organizations find it convenient or even necessary to adopt a bring your own device (BYOD) policy that allows the personal mobile devices of employees to have access to corporate resources. IT managers should be able to inspect each device before allowing network access. IT should establish configuration guidelines for operating systems and applications. For example, rooted or jailbroken devices are not permitted on the network, and mobile devices cannot store corporate contacts on local storage. Whether a device is owned by the organization or an employee, the organization should configure the device with security controls, including taking the following measures:

- Enable auto-lock, which causes the device to lock if it has not been used for a given amount of time, requiring the user to reenter a PIN or a password to reactivate the device.
- Enable password or PIN protection. The PIN or password is needed to unlock the device. In addition, it can be configured so that email and other data on the device are encrypted and can be retrieved only with the PIN or password.
- Avoid using auto-complete features that remember usernames or passwords.
- Enable remote wipe.
- Ensure that Transport Layer Security/Secure Sockets Layer (TLS/SSL) protection is enabled, if available.
- Make sure that software, including operating systems and applications, is up to date.
- Install antivirus software as it becomes available.
- Either prohibit users from storing sensitive data on mobile devices or require users to encrypt sensitive data.

https://t.me/learningnets

- Ensure that IT staff have the ability to remotely access devices, wipe devices of all data, and disable devices in the event of loss or theft.
- Possibly prohibit installation of third-party applications, implement whitelisting to prohibit installation of all unapproved applications, or implement a secure sandbox that isolates the organization's data and applications from all other data and applications on the mobile device. Any application that is on an approved list should be accompanied by a digital signature and a public-key certificate from an approved authority.
- Implement and enforce restrictions on what devices can synchronize and on the use of cloud-based storage.
- To deal with the threat of untrusted content, disable camera use on corporate mobile devices and train personnel on the risks inherent in untrusted content.
- To counter the threat of malicious use of location services, ensure that such services are disabled on all mobile devices.

Mobile Applications

Millions of apps are available from the two major stores, the Apple App Store and Google Play, and millions more can be obtained from other public app stores. The reliability and security of apps may vary widely, and the vetting process may be opaque or insufficiently robust, particularly for apps from outside the two major stores.

Regardless of the source of an app, an enterprise should perform its own evaluation of the security of the app to determine if it conforms to the organization's security requirements. The requirements should specify how data used by the app should be secured, the environment in which the app will be deployed, and the acceptable level of risk for the app.

Figure 7.6 illustrates *app vetting*, the process of evaluating and either approving or rejecting apps within an organization, which is described in NIST SP 800-163, *Vetting the Security of Mobile Applications*. The vetting process begins when an app is acquired from a public or enterprise store or submitted by an in-house or third-party developer. An administrator is a member of the organization who is responsible for deploying, maintaining, and securing the organization's mobile devices as well as ensuring that deployed devices and their installed apps conform to the organization's security requirements. The administrator submits the app to an app testing facility in the organization that employs automated and/or human analyzers to evaluate the security characteristics of apps, including searching for malware, identifying vulnerabilities, and assessing risks. The resulting security report and risk assessment are conveyed to an auditor or auditors.

https://t.me/learningnets

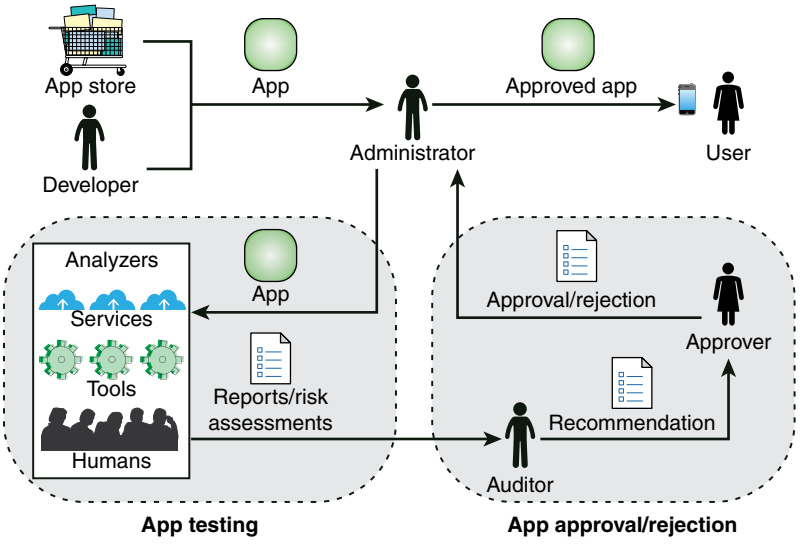


FIGURE 7.6 App Vetting Process

AppVet
http://appvet.github.io/appvet/

The role of the auditor is to inspect reports and risk assessments from one or more analyzers to ensure that an app meets the security requirements of the organization. The auditor also evaluates additional criteria to determine if the app violates any organization-specific security requirements that could not be ascertained by the analyzers. The auditor then makes a recommendation to someone in the organization who has the authority to approve or reject an app for deployment on mobile devices. If the approver approves an app, the administrator can then deploy the app on the organization's mobile devices.

NIST has developed a tool, AppVet, that provides automated management support for app testing and app approval/rejection activities

Mobile Network Protocols and Services

Traffic security is based on the usual mechanisms for encryption and authentication. All traffic should be encrypted and travel by secure means, such as SSL or IP Security (IPsec). **Virtual private networks (VPNs)** can be configured so that all traffic between a mobile device and the organization's network is via a VPN.

virtual private network (VPN)
A restricted-use, logical (that is, artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (that is, real) network (for example, the Internet), often using encryption (located at hosts or gateways) and authentication. The endpoints of the virtual network are said to be tunneled through the larger network.

https://t.me/learningnets

A strong authentication protocol should be used to limit access from the device to the resources of the organization. Often, a mobile device has a single device-specific authenticator because it is assumed that the device has only one user. A preferable strategy is to have a two-layer authentication mechanism, which involves authenticating the device and also authenticating the user of the device.

The organization should have security mechanisms to protect the network from unauthorized access. The security strategy can also include firewall policies specific to mobile device traffic. Firewall policies can limit the scope of data and application access for all mobile devices. Similarly, intrusion detection and intrusion prevention systems can be configured with tighter rules for mobile device traffic.

Physical Access to the Device

side-channel attack
An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions.

The small, portable nature of mobile devices increases their susceptibility to physical-based threats. The DHS's *Study on Mobile Device Security* [DHS17] lists the following as common threats resulting from gaining physical access to a device:

- Substitution of a compromised Bluetooth headset to facilitate eavesdropping
- Replacement of a SIM card to facilitate illegal activity such as identity fraud or theft of services
- Brute-force attacks on a stolen device
- **Side-channel attacks** to obtain cryptographic private keys
- Installation of malicious apps via USB, an infected computer, or a charging station without the user's knowledge

The DHS report recommends the following defenses [DHS17]:

screen lock
A security feature for computers and mobile devices that helps prevent unauthorized access to the device. A screen lock requires the user to perform a specific action, such as entering a PIN code or presenting a fingerprint, to gain access to the device.

- Ensure that devices are enterprise managed so that the organization can enforce security policies, monitor device state, and remotely track or wipe lost or stolen devices.
- Ensure that the device's **screen lock** is enabled. The lock should be enabled with an appropriately strong password.

Enterprise Mobile Infrastructure

Attacks on mobile devices with enterprise access can spread to other enterprise systems. As shown in Figure 7.5, these enterprise threats are in two broad areas: attacks related to an enterprise app store and attacks on the EMM system.

https://t.me/learningnets

If the enterprise app store facility is not fully secure, it may be possible for an adversary to bypass the vetting process and introduce apps with malware delivered to devices from the enterprise app store. Such malware can target the mobile device or can be used to spread malware to other platforms in the enterprise.

Attacks on the EMM system can be devastating. Because EMM systems have elevated privileges, intruders can leverage control over EMMs to launch attacks against mobile devices and the mobile enterprise. An attacker may steal administrative credentials or exploit vulnerabilities in the EMM infrastructure or software to gain unauthorized access to the administrative console and launch attacks against mobile devices. Defenses against such attacks can include security audits, threat intelligence, strong authentication, and secure network connections.

Resources for Mobile Device Security

A number of documents for U.S. agencies are valuable resources for any organization. The following are particularly useful:

- ***Study on Mobile Device Security* [DHS17]:** Develops a threat model consisting of six areas and provides a detailed summary of the greatest threats in each area as well as current mitigations and defenses.
- **NIST IR 8144, *Assessing Threats to Mobile Devices & Infrastructure*:** Provides a detailed description of the threats related to mobile devices and the enterprise.
- **SP 800-124, *Guidelines for Managing and Securing Mobile Devices in the Enterprise*:** Provides recommendations for selecting, implementing, and using centralized management technologies, explains the security concerns inherent in mobile device use, and provides recommendations for securing mobile devices throughout their life cycles.
- **SP 800-163, *Vetting the Security of Mobile Applications*:** Describes in detail app vetting and app approval/rejection activities.
- **SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*:** Focuses on defining the fundamental security primitives and capabilities needed to securely enable mobile devices.
- **SP 1800-4, *Mobile Device Security: Cloud and Hybrid Builds*:** Contains reference architectures; demonstrates implementation of standards-based, commercially available cybersecurity technologies; and helps organizations use technologies to reduce the risk of intrusion via mobile devices.

https://t.me/learningnets

7.5 Physical Asset Management Best Practices

The SGP breaks down physical asset management best practices into two areas and eight topics and provides detailed checklists for each topic. These are the areas and topics:

- **Equipment management:** The objective of this area is to protect physical assets, including systems and network equipment, office equipment (for example, network printers, MFDs), and specialist equipment (for example, industrial control systems) throughout their life cycles, and to address the information security requirements for the acquisition (for example, purchase or lease), maintenance, and disposal of equipment.
  - **Hardware life cycle management:** The SGP details procedures for ensuring not only that hardware provides the required functionality but that security policy is observed and its risk managed throughout the life cycle of the equipment. The SGP checklists provide guidance for selecting hardware, identifying potential security weaknesses, maintaining a register of hardware assets, tracking hardware through its life cycle, and securely disposing of hardware.
  - **Office equipment:** Additional security-related measures are needed for office equipment. The SGP covers a number of issues, including physical protection, access control, monitoring use, and encryption of transmitted information.
  - **Industrial control systems:** Information systems that monitor or control physical activities should be identified, categorized, and protected by security arrangements that are tailored to operate in those environments. The SGP discusses risk assessment and security control selection tailored to industrial control systems.
- **Mobile computing:** The objective of this area is to protect mobile devices (including laptops, tablets, and smartphones) and the information they handle against unauthorized disclosure, loss, and theft.
  - **Mobile device configuration:** The SGP details procedures for using standard, technical configurations and security management practices.
  - **Enterprise mobility management:** The SGP provides a checklist of capabilities for an EMM to protect against losses, threats, and cyber attacks.

https://t.me/learningnets

- **Mobile device connectivity:** Techniques to ensure secure connectivity include proper configuration and use of authentication and VPNs between the device and the enterprise network.
- **Employee-owned devices:** The SGP specifies using documented agreements with staff and technical security controls to protect business information.
- **Portable storage devices:** The SGP describes policies for portable storage devices in the areas of approval, restricted access, and data protection.

7.6 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

app store
application whitelisting
attack surface
configuration management
configuration management database (CMDB)
cryptographic erasure
denial-of-service (DoS) attack
enterprise mobility management (EMM)
golden record
hardware
hardware asset management
hardware life cycle management
industrial control system (ICS)
jailbreaking
least privilege
mobile device
multifactor authentication (MFA)
multifunction device
office equipment
physical asset
rooting
screen lock
self-encrypting drive (SED)
side-channel attack
sideloading
virtual private network (VPN)

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Enumerate and briefly describe the four subtopics of physical asset management, according to the SGP.
2. Which three subcategories of assets are considered part of hardware, according to the SGP?
3. What factors advocate for adoption of a well-drafted hardware life cycle management policy?

https://t.me/learningnets

4. Explain the steps that an organization must follow to develop an ideal acquisition system for hardware assets.
5. What is the best way to manage hardware equipment after its deployment?
6. Describe three potential sources of vulnerabilities in MFDs.
7. Define *media sanitization* and list three actions for sanitization.
8. List and describe the principal elements of an ICS.
9. How do IT systems differ from ICSs in terms of performance requirements?
10. List typical security threats to an ICS.
11. What does the term *mobile device technology stack* mean?
12. According to SP 800-14, what are the major security concerns related to mobile devices?
13. What is AppVet?

7.7 References

CIS09: Center for Internet Security, *Security Benchmark for Multi-Function Devices*. April 2009. https://www.cisecurity.org.

CREN17: Crenshaw, A., "Hacking Network Printers." http://www.irongeek.com/i.php?page=security/networkprinterhacking.

DHS10: U.S. Department of Homeland Security and the U.K. Centre for the Protection of National Infrastructure, *Cyber Security Assessments of Industrial Control Systems.* November 2010.

DHS11: U.S. Department of Homeland Security, *Catalog of Control Systems Security: Recommendations for Standards Developers.* Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, April 2011.

DHS15: U.S. Department of Homeland Security, *Seven Steps to Effectively Defend Industrial Control Systems*. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, December 2015.

DHS16: U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, September 2016.

https://t.me/learningnets

DHS17: U.S. Department of Homeland Security, *Study on Mobile Device Security*. DHS Report, April 2017.

GARR10: Garretson, C., "Pulling the Plug on Old Hardware: Life-Cycle Management Explained." *ComputerWorld*, April 22, 2010.

IAIT12: The International Association of Information Technology Asset Managers, *What Is IT Asset Management?* White paper, 2012.

IBM14: IBM, *IBM Predictive Maintenance and Quality (Version 2.0).* IBM Redbooks Solution Guide, 2014.

SCHN14: Schneier, B., "The Internet of Things Is Wildly Insecure—And Often Unpatchable." *Wired*, January 6, 2014.

SCOT07: Scott, C., "Auditing and Securing Multifunction Devices." *SANS Institute*, January 25, 2007.

https://t.me/learningnets

Chapter 8

System Development

It should be stated at the outset that we are dealing with an extremely complicated system and one that is even more complicated to describe. It would be treacherously easy for the casual reader to dismiss the entire concept as impractically complicated. The temptation to throw up one's hands and decide that it is all "too complicated" should be deferred until the fine print has been read.

—*On Distributed Communications*, Rand Report RM-3420-PR, Paul Baran, August 1964

Learning Objectives

After studying this chapter, you should be able to:

- Explain in detail the National Institute of Standards and Technology (NIST) system development life cycle model.
- Present an overview of DevOps.
- For each of the phases of the NIST SDLC model, describe the security measures that should be incorporated.
- Understand the concept and functions of system development management.
- Present an overview of system development best practices.

8.1 System Development Life Cycle

The **system development life cycle (SDLC)** is the overall process of developing, implementing, and retiring information systems. Various SDLC models have been developed to guide the processes involved, and some methods work better than others for specific types of projects. The following sections examine several alternative models.

https://t.me/learningnets

NIST SDLC Model

Figure 8.1 illustrates the SDLC model defined in NIST SP 800-64, *Security Considerations in the System Development Life Cycle*. Although this model is depicted as a cycle, it is more accurately defined as a linear sequence that uses the **waterfall development** methodology. The following sections discuss the phases in this model.

waterfall development
A method of deploying software or systems in which development moves through a series of fairly well-defined stages. With large projects, once each stage is completed, it cannot be easily reversed, much as it would be difficult to move up a waterfall. This traditional system engineering flow allows for a requirements-driven process that leads to assured and verified function.

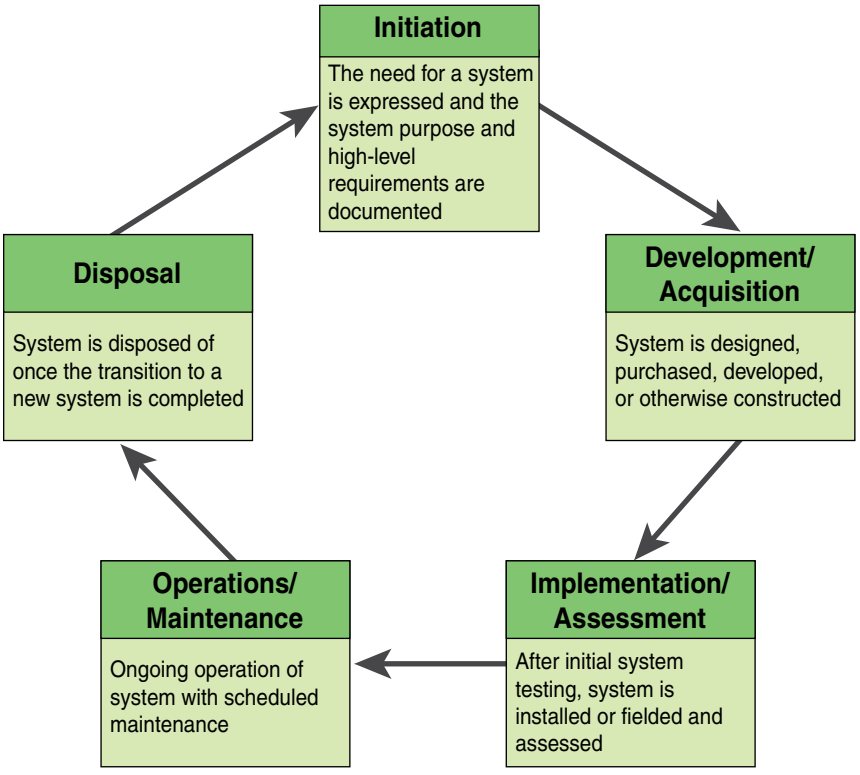


FIGURE 8.1 NIST System Development Life Cycle

Initiation Phase

During the initiation phase, the responsible individual or group documents the purpose of the system and defines the requirements. During the initiation phase, the organization establishes the need for a particular system and documents its purpose. The information to be processed, transmitted, or stored is typically evaluated, along with who needs access to such information and how (in high-level terms). In addition, it is often determined whether the project will be an independent information system or a component of an already-defined system.

https://t.me/learningnets

Specific parts of this phase include the following:

- **Strategy:** Ensure that the system release is fully aligned to the master strategy and intent. System or asset owners work with appropriate stakeholders to develop a high-level strategy or roadmap of work, outlining the details of a specific system release.
- **Research:** Determine opportunities and solution options that meet requirements.
- **Feasibility:** If the overall strategy is acceptable to management, then the next step is to examine the feasibility of the system. Key considerations include:
  - **Economic feasibility:** Determine whether the likely benefits of the system outweigh the cost, using a cost/benefit analysis.
  - **Operational feasibility:** Determine whether the proposed system will in fact satisfy system requirements as defined for the user's environments.
  - **Organizational feasibility:** Determine whether the proposed system is consistent with the organization's strategic objectives.
  - **Technical feasibility:** Determine whether the available technology and resources are adequate to implement the proposed system.
  - **Social feasibility:** Determine whether the proposed system will produce unwanted society impacts.
- **Planning:** Carry out activities such as detailing what will actually go into the system release (for example, new features and fixes), creating initial project plans, and improving budget estimates.
- **Requirements:** Develop a requirements specification of what needs to be accounted for in downstream design and implementation activities. The more detailed the requirements, the higher the probability that the design will align to the intended system release strategy and with end-user expectations for the release.

Development/Acquisition Phase

During the development/acquisition phase, the system is designed, purchased, programmed, developed, or otherwise constructed. Specific parts of this phase typically include the following:

- **Design:** The detailed design is performed to respond to requirements. In addition to designing the operational solutions associated with functional and non-functional requirements, the design process also includes designing unit, module, integration, user acceptance, and production signoff tests that will be used to verify the quality of all work performed in all downstream phases and environments.

https://t.me/learningnets

- **Procurement or coding:** The detailed design of a system release is realized and optimized, with the intent that it will be handed off for a centralized and repeatable build that can be used for distribution/deployment, quality assurance, and signoff in downstream phases and environments.
- **Centralized build:** A build team creates a fully centralized, repeatable, and automated build that will be used for distribution/deployment, quality assurance, and signoff in downstream phases and environments.
- **Integration testing:** All data and technology connections are tested for a specific system moving through the SDLC and all of its upstream system dependencies (that is, systems that provide data to the system being tested) and all of its downstream system targets (that is, systems to which the system being tested provides data). The goal is to verify all appropriate data connections and data exchanges between systems that will need to interact in the final operating environment.
- **Documentation:** Generally, two types of documentation are prepared for the system:
  - **User documentation:** User documentation provides a complete description of the system from the user's point of view, detailing how to use or operate the system. It also includes the major error messages likely to be encountered by the user.
  - **System documentation:** System documentation contains the details of system design, programs, their coding, system flow, data dictionary, process description, and so on. This helps in understanding the system and permitting changes to be made in the existing system to satisfy new user needs.
- **User acceptance testing (UAT):** This testing is targeted at system functions that end users will be able to execute while operating in the final production environment. Such testing ensures that what an end user does or sees meets appropriate quality expectations.

Implementation/Assessment

After the system development phase, the implementation phase begins. Implementation is the stage of a project during which theory is turned into practice. The major parts of this phase are:

- **Installation of hardware and software:** The hardware and the relevant software required for running the system must be made fully operational.
- **Conversion:** The data need to be converted from the old system to operate in the new format of the new system. During this part of the process, all the programs of the system are loaded onto the user's computer.

https://t.me/learningnets

- **User training:** The main topics of user training can include how to execute the package, how to enter data, how to process data, and how to generate reports.
- **Changeover:** If the new system replaces an existing IT system or even a manual system, the organization needs to shift the work from the old system to the new. Three basic strategies are possible:
  - **Direct changeover:** The old system is completely replaced by the new system. This is a risky approach and requires comprehensive system testing and training.
  - **Parallel run:** The two systems are executed simultaneously for a certain defined period, and the same data are processed by both the systems. This strategy is less risky but more expensive.
  - **Pilot run:** The new system is run with the data from one or more of the previous periods for the whole system or part of it. The results are compared with the old system results. This is less expensive and risky than the parallel run approach. This strategy builds confidence and allows for error tracing without affecting operations.

Operations/Maintenance

This phase involves maintenance, replacement of outdated or malfunctioning hardware and software, and regular software updates. This phase also involves monitoring and evaluation to determine whether requirements are being met and what is in need of improvement. This can mean recommending additional training, operations, procedures, or upgrades.

Disposal

The disposal phase of the system life cycle refers to the process of preserving (if applicable) and discarding system information, hardware, and software. Disposal of data assets is discussed in Chapter 6, "Information Management," and disposal of physical assets is discussed in Chapter 7, "Physical Asset Management."

The SGP's SDLC Model

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) defines the SDLC in terms of 10 stages (see Figure 8.2):

https://t.me/learningnets

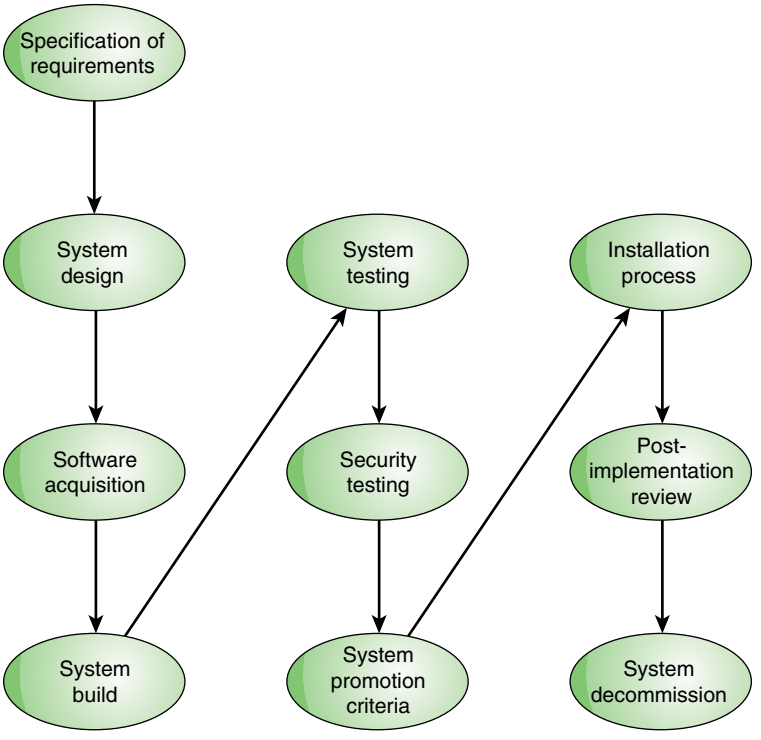


FIGURE 8.2 SGP System Development Life Cycle

1. **Specifications of requirements:** The design may cover requirements in the areas of performance (for example, processing speeds, response times), capacity (for example, number of users, volume and size of transactions), continuity (for example, maximum length of time to recover key components following a system failure/outage), scalability (for example, to support future developments or changes), connectivity (for example, interfaces to existing systems, networks, or external resources), and compatibility (for example, with particular technical environments or components).
2. **System design:** The design should include the necessary hardware and/or software specifications. In addition, the design phase should involve analysis of the information life cycle in systems under development.
3. **Software acquisition:** The objective of this phase is to acquire (purchase or lease) robust, reliable software. Software should be acquired from approved suppliers and covered by adequate support and maintenance agreements.

https://t.me/learningnets

4. **System build:** System build activities (including program coding and software package customization) should be carried out in accordance with industry good practice, performed by individuals provided with adequate skills/tools, and inspected to identify unauthorized modifications or changes.
5. **System testing:** Systems under development (including application software packages, system software, hardware, communications, and services) should be tested in a dedicated testing area that simulates the live environment before the system is promoted to the live environment.
6. **Security testing:** Systems under development should be subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing, and access control testing).
7. **System promotion criteria:** Rigorous criteria (including security requirements) should be met before new systems are promoted into the live environment.
8. **Installation process:** New systems should be installed in the live environment in accordance with a documented installation process.
9. **Post-implementation review:** Once operational, a system should be subject to early review to ensure that it operates as intended.
10. **System decommission:** System disposal should be carried out according to organization policy.

The SGP model is finer-grained, with somewhat different emphases, than the NIST model, but the basic concepts are the same.

DevOps

DevOps
A contraction of development and operations that refers to the tight integration between the developers of applications and the IT department that tests and deploys them. DevOps is said to be the intersection of software engineering, quality assurance, and operations.

In just a few short years, **DevOps** has gone from being a buzzword to being an accepted method of software development and deployment. Enterprises large and small are trying to get a grasp on what DevOps is and the impact it can have on their organizations. The attention is coming not just from IT executives and CIOs but also from business managers who are beginning to recognize the potential of DevOps to enable business units to become more efficient, deliver higher-quality products, and be more agile and innovative. Major software organizations, including IBM and Microsoft, are rapidly expanding their DevOps offerings.

The focus of DevOps has been the development of application software and support software. The essence of the DevOps philosophy is that all participants in creating a product or system should collaborate from the beginning, including business unit managers, developers, operations staff, security staff, and end-user groups.

https://t.me/learningnets

To understand the DevOps approach, let's briefly look at the typical stages in the development and deployment of applications. As described in *Application Release and Deployment for Dummies*, most application vendors and in-house application developers follow a life cycle similar to the following [MINI14]:

1. **Development:** Developers build and deploy code in a test environment, and the development team tests the application at the most basic level. The application must meet certain criteria for advancement to the next phase.
2. **System integration testing:** The application is tested to ensure that it works with existing applications and systems. The application must meet the criteria of this environment before it can move to the next phase.
3. **User acceptance testing:** The application is tested to ensure that it provides the required features for end users. This environment is usually production-like. The application must pass these requirements to move to the next phase.
4. **Production:** The application is made available to users. Feedback is captured by monitoring the application's availability and functionality. Any updates or patches are introduced in the development environment to repeat this cycle.

A traditional information system development project proceeds sequentially through these stages, without delivering working pieces in between and without obtaining customer feedback on the way. This process is called waterfall development. As mentioned earlier in this chapter, with large projects, once each stage is completed, it cannot be easily reversed. Beginning in the early 2000s, *Agile software development* began to gain favor. Agile emphasizes teamwork, customer involvement, and, most significantly, the creation of small or partial pieces of the total system that are tested in a user environment. For example, an application with 25 features might be prototyped with only 5 or 6 features thoroughly completed before more are added. Agile development has proven to be more effective for dealing with the changing requirements that tend to occur during the development phase.

Agile development is characterized by frequent releases, in an iterated loop fashion, with a certain amount of automation in the form of tools that can be used to support collaboration. DevOps takes this philosophy much further. It is characterized by rapid releases, feedback loops embedded throughout the process, and a comprehensive set of tools and documented best practices to automate the DevOps process.

Figure 8.3, based on *DevOps for Dummies* [SHAR15], provides an overview of the DevOps process.

https://t.me/learningnets

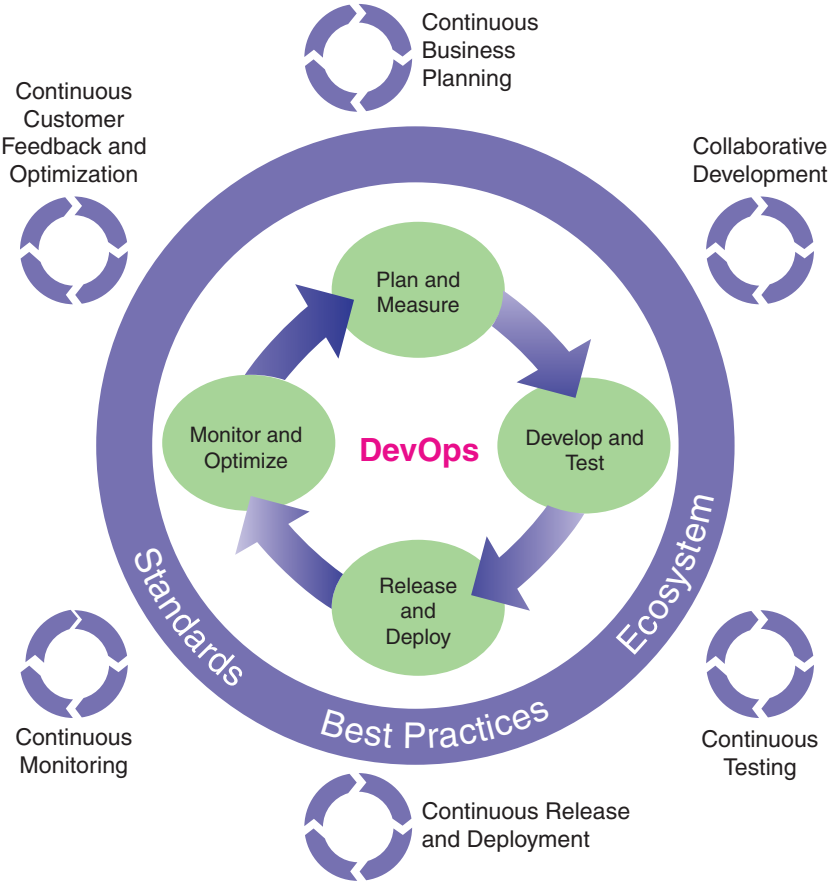


FIGURE 8.3 DevOps Reference Architecture

DevOps is viewed as a repetitive cycle of four major activities:

- **Plan and measure:** This activity focuses on business units and their planning process. The planning process relates business needs to the outcomes of the development process. This activity can start with small, limited portions of the overall plan, identifying outcomes and resources needed to develop the required software. The plan must include developing measures that are used to evaluate software, adapt and adjust continually, relate to customer needs, and continually update the development plan and the measurement plan. The measurement function can also be applied to the DevOps process itself to ensure that the right automated tools are being used and that collaboration is ongoing.
- **Develop and test:** This activity focuses on collaborative development, continuous integration of new code, and continuous testing. It focuses on streamlining

https://t.me/learningnets

development and testing teams' capabilities. Useful tools are automated tracking of testing against measured outcomes and virtualized test beds that enable testing in an isolated but real-world environment.

- **Release and deploy:** This activity provides a continuous delivery pipeline that automates deployment to test and production environments. Releases are managed centrally in a collaborative environment that leverages automation. Deployments and middleware configurations are automated and then mature to a self-service model that provides individual developers, teams, testers, and deployment managers with the capability to continuously build, provision, deploy, test, and promote. Infrastructure and middleware provisioning evolves to an automated and then self-service capability similar to that for application deployment. Operations engineers cease manually changing environments; instead, they focus on optimizing the automation.
- **Monitor and optimize:** This activity includes the practices of continuous monitoring, customer feedback, and optimization to monitor how applications are performing post-release, allowing businesses to adapt their requirements as needed. Customer experience is monitored to optimize experiences in business applications. Optimization to customer key performance indicators that reflect business value attainment is part of the continuous improvement program.

Figure 8.4, based on figures in the Microsoft white paper *Enterprise DevOps* [MICR15], provides another useful perspective on DevOps. DevOps is intended to improve the efficiency and effectiveness of the process of managing applications throughout their life cycles. With the introduction of Agile software development, organizations have developed **application life cycle management (ALM)** practices to integrate the business, development, quality assurance, and operations functions in a virtuous cycle for greater agility in delivering continuous value.

application life cycle management (ALM)
The administration and control of an application from its inception to its demise. ALM embraces requirements management, system design, software development, and configuration management, and implies an integrated set of tools for developing and controlling the project.

As Figure 8.4a shows, ALM practices, as they have developed, have encountered a number of impediments to effective delivery of the final product. These impediments arise from the conventional divide that exists between the development and operations functions. A key theme illustrated here is the danger that operations requirements are being deprioritized to accommodate functional needs. DevOps intends to address these impediments, as shown in Figure 8.4b.

Fundamentally, DevOps rests on two key foundations: collaboration and automation. Collaboration begins with management policy to encourage and require the various actors in the software development and deployment process to work together. Automation consists of tools that support that collaboration and are designed to automate as much as possible the cyclic process illustrated in Figures 8.3 and 8.4.

https://t.me/learningnets

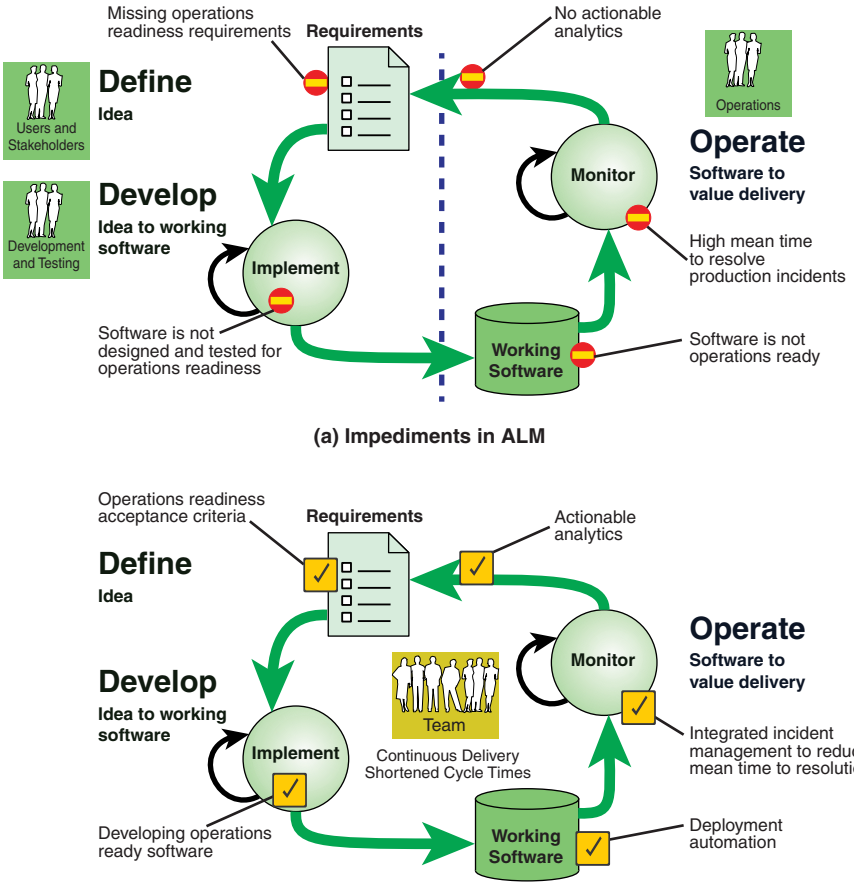


FIGURE 8.4 Modern Application Life Cycle Management

A number of companies now offer DevOps automation tools. For example, Microsoft has a number of tools that work as part of Visual Studio. Visual Studio is a set of developer tools and services to assist users in creating apps on Microsoft platforms and in the cloud. One of the additions is release management software that automates many of the chores required to move a software program from development to production, such as alerting the appropriate managers and preparing the production server to run the software. Another DevOps-minded feature Microsoft has introduced for Visual Studio, Cloud Deployment Projects, allows organizations to capture and reuse the configuration settings of new applications in order to speed the deployment times. The configuration settings, or blueprints, are captured within a virtual machine (VM), which then can be deployed, holding the application in the Microsoft Azure cloud. In addition, Microsoft's Application Insights software provides a way to instrument an

https://t.me/learningnets

application so developers can determine if it is working correctly and also see how people are using the software program. This may help developers pinpoint bugs, as well as get early insight into behavioral issues, such as a sudden fall-off of use due to a poor redesign.

8.2 Incorporating Security into the SDLC

Enterprise security considerations dictate that security-focused activities and deliverables be a part of every phase of the SDLC in order to ensure that the developed system is able to withstand malicious attacks. Whatever SDLC methodology is used, an enterprise should make sure both that the SDLC methodology lends itself to a comprehensive security component and that security policies and procedures are well defined for each phase.

This section examines the considerations for incorporating security into the SDLC using the NIST SDLC model (refer to Figure 8.1). It should be clear how this security strategy could also be applied to a finer-grained or otherwise different SDLC methodology, including DevOps.

SP 800-64 lists the following as benefits of integrating security into the SDLC:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation
- Awareness of potential engineering challenges caused by mandatory security controls
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques
- Facilitation of informed executive decision making through the application of comprehensive risk management in a timely manner
- Documentation of important security decisions made during development, ensuring management that security was fully considered during all phases
- Improved organization and customer confidence to facilitate adoption and use as well as improved confidence in the continued investment in system development
- Improved systems interoperability and integration that would be difficult to achieve if security were considered separately at various system levels

https://t.me/learningnets

SP 800-64 makes use of the following elements in defining the security considerations applied during each phase:

- **Major security activities:** During each phase, a number of security-related activities are needed to assure that security is incorporated effectively in that design phase.
- **Expected outputs:** A key to the success of incorporating security into the SDLC is to define specific deliverables for each activity.
- **Synchronization:** A feedback loop between tasks provides opportunities to ensure that the SDLC is implemented as a flexible approach that allows for appropriate and consistent communication and the adaptation of tasks and deliverables as the system is developed.
- **Control gates:** Control gates are decision points at the end of each phase when the system is evaluated and when management determines whether the project should continue as is, change direction, or be discontinued.

Initiation Phase

Figure 8.5 illustrates the relationships among five key security-related activities that comprise the initiation phase. During this initial phase, the security focus is on identifying and assessing risks.

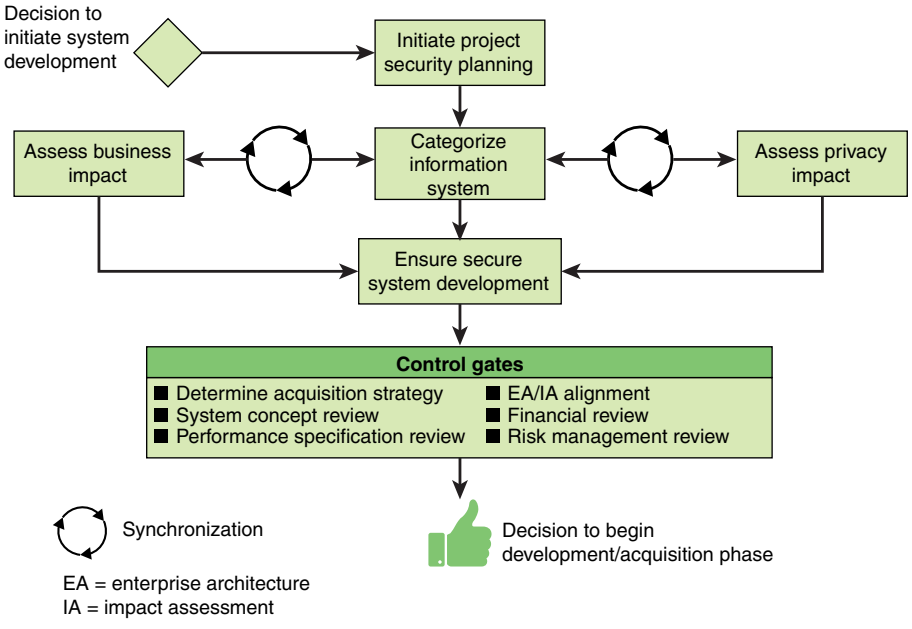


FIGURE 8.5 Security in the Initiation Phase

https://t.me/learningnets

Initiating Project Security Planning

While initiating project security planning, the key security roles that will be active throughout the SDLC should be identified. In addition, the **system owner** needs to identify the standards and regulations that apply and develop an overall plan for security milestones during system development. It is also important to ensure that all key stakeholders have a common understanding, including security implications, considerations, and requirements. This planning activity enables developers to design security features into the project.

system owner
A person or an organization that has responsibility for the development, procurement, integration, modification, operation, maintenance, and final disposition of an information system.

An expected output of this activity is a set of supporting documents that provide a record of the agreed-upon planning decisions. Another key output is an initial set of security activities and decisions related to the SDLC.

Categorizing Information Systems and Assessing Impact

Categorizing information systems corresponds to step 1 in the NIST risk management framework defined in SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (refer to Figure 6.1 in Chapter 6). The purpose is to identify information that will be transmitted, processed, or stored by the system and to define applicable levels of information categorization based on an impact analysis. This categorization process depends initially on business and privacy impact assessments and should be revisited if there are updates to either of these assessments.

The result of this step should be an information taxonomy or catalog of information types. The level of detail, or granularity, must be determined by those involved in security governance. The decision may be based on factors such as the size of the organization, its range of activities, and the perceived overall level of risk.

The expected outputs of this activity include supporting rationale for the information system security categorization and a level of effort estimate for applying the necessary security controls, together with a specification of security requirements.

Assessing business impact synchronizes with the categorization activity. An assessment of system impact on lines of business correlates specific system components with the critical business services that are provided. That information is then used to characterize the business and mission consequences of a disruption to the system's components. Output from this activity includes a statement of the lines of business that are supported or otherwise impacted by the system under design and the level of tolerance for downtime and data loss.

Assessing privacy impact also synchronizes with the categorization activity. This assessment focuses on personally identifiable information (PII) and is essentially a two-step activity. First, the system owner should determine if, and to what extent, the system under design will process, store, or create PII. Then the system owner should work toward identifying proper safeguards and security controls, including processes

https://t.me/learningnets

to address privacy information incident handling and reporting requirements. The output from this activity is a privacy impact assessment that provides details on where and to what degree PII is collected, stored, or created within the system.

A key result of the process of categorizing information systems and assessing business and privacy impacts should be a set of security requirements that are to be incorporated into the overall set of requirements for the system. ISO 27002, *Code of Practice for Information Security Controls*, suggests that the security requirements consider the following:

- The level of confidence required toward the claimed identity of users, in order to derive user authentication requirements
- Access provisioning and authorization processes for business users as well as for privileged or technical users
- User and operator knowledge of their duties and responsibilities
- The required protection needs of the assets involved, especially regarding availability, confidentiality, and integrity
- Requirements derived from business processes, such as transaction logging and monitoring as well as non-repudiation requirements
- Requirements mandated by other security controls, such as interfaces to logging and monitoring and data leakage detection systems

Ensuring Secure System Development

The system owner and the development team should work together to develop a set of principles and plans that document security expectations throughout the SDLC. These considerations include:

- **Secure concept of operations:** The team should define the overall concept and guidelines for secure development and deployment in the target environment. The team should define the characteristics of a source code repository that will preserve the source code work product in the event of interruption to the development environment.
- **Standards and processes:** The team should document which standards and best practices will be followed, in order to assure development conforms to organizational expectations.
- **Security training for development team:** The team should determine what additional security training should be provided for key developers to understand the current threats and potential exploitations of their products, as well as training for secure design and coding techniques.

https://t.me/learningnets

- **Quality management:** The team should define a quality management protocol (which includes planning, assurance, and control) to ensure minimal defects within and proper execution of the information system.
- **Secure environment:** The team must ensure that the development environment, including workstations, servers, network devices, and code repositories, meets the organization's security requirements.
- **Secure code practices and repositories:** Special attention should be placed on code repositories, with an emphasis on systems that support distributed code contribution with check-in/check-out functionality. Role-based access should apply to accessing the code repository, and logs should be reviewed regularly as part of the secure development process. When possible, completed software components that have passed security certification should be retained as reusable components for future software development and system integration.

source code repository

A database of source code, typically used for projects involving a large number of developers and/or to store code that may be used on a number of projects. A repository may be private to an organization or public. Public repositories may be open source or restricted to developers from multiple organizations. Repositories help developers submit patches of code in an organized fashion. Often these archives support version control, bug tracking, release management, mailing lists, and wiki-based documentation.

The output from this activity should include plans for development phase security training and quality assurance.

Control Gates

The initiation phase involves the following control gates:

- **Determine acquisition strategy:** To be used through the remainder of the SDLC
- **System concept review:** To verify that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints
- **Performance specification review:** To ensure that the initial design meets all security requirements
- **EA/IA (enterprise architecture/information architecture) alignment:** To determine that the enterprise architecture (see Chapter 2, "Security Governance") incorporates the business impact and privacy impact requirements generated for this system development
- **Financial review:** To determine that the system aligns with capital planning considerations, balancing cost implications with risk management
- **Risk management review:** To ensure that the review follows the NIST risk management framework defined in SP 800-37 (refer to Figures 6.1 and 6.2 in Chapter 6) or similar methodology to ensure that risk is managed properly for this system development

https://t.me/learningnets

Development/Acquisition Phase

Figure 8.6 illustrates the relationships among six key security-related activities that comprise the development/acquisition phase. A key security activity in this phase is conducting a risk assessment and using the results to supplement the baseline security controls. In addition, an organization should analyze security requirements, perform functional and security testing, prepare initial documents for system certification and accreditation, and design the security architecture.

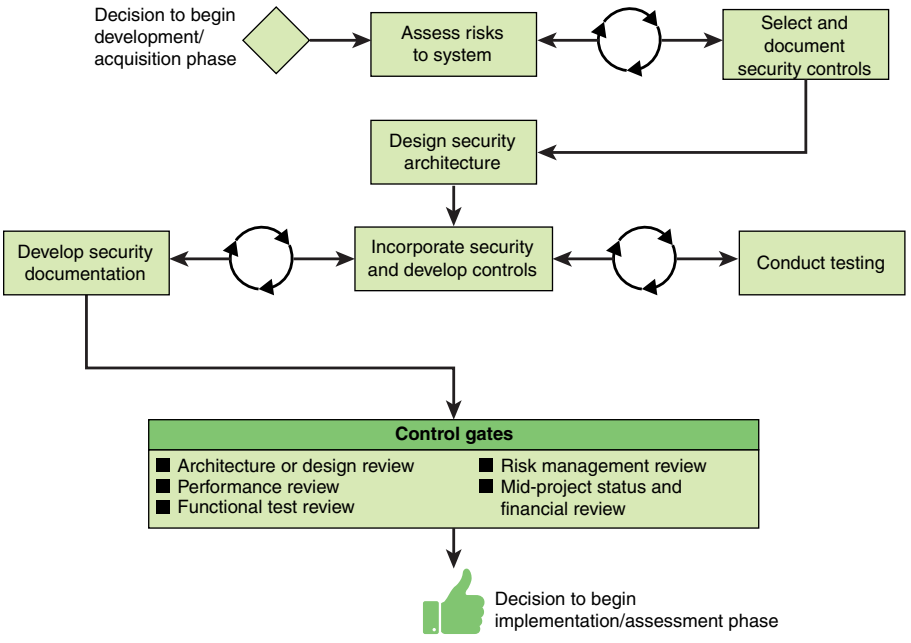


FIGURE 8.6 Security in the Development/Acquisition Phase

Assessing Risks and Selecting Controls

A risk assessment enables an organization to determine the risk to operations, assets, and individuals resulting from the operation of information systems and the processing, storage, or transmission of information.

The risk assessment activity looks at the current knowledge of the systems design and the impact assessment information from the initiation phase. The results are used to supplement baseline security controls identified during the initiation phase. The expected output is a refined risk assessment based on a more mature system design that more accurately reflects the potential risk to the system, known weaknesses in the design, identified project constraints, and known threats to both business and IT components.

https://t.me/learningnets

Selecting and documenting security controls corresponds to step 2 in the NIST risk management framework defined in SP 800-37 (refer to Figures 6.1 and 6.2 in Chapter 6) and should synchronize with the risk assessment activity. Typically, a baseline set of controls is selected and then adjusted with additional controls, based on a refinement of the risk assessment. The refinement takes into account any possible secondary risks that result from the baseline controls and how they affect the risk assessment. The output is a system security plan. Recall from Chapter 4, "Security Management," that a security plan is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. Key components of the plan are a security categorization, which gives the acceptable level of risk for each distinct element of the system, and a description of each security control plus its implementation plan.

Designing the Security Architecture

This security architecture design activity produces a detailed architecture that incorporates security features and controls into the system design. Expected outputs include:

- A schematic of security integration that provides details on where within the system security is implemented and shared
- A list of shared services and resulting shared risk
- Identification of common controls used by the system

Developing, Testing, and Documenting Security Controls and Features

During the last part of the development, testing, and documentation phase, security controls are implemented and become part of the system. This corresponds to step 3 in the NIST risk management framework defined in SP 800-37 (refer to Figures 6.1 and 6.2 in Chapter 6). As part of implementation, the organization should perform developmental testing of the technical and security features/functions to ensure that they perform as intended prior to launching the implementation and integration phase. The security controls may be modified at this point as a result of **functional testing**, **penetration testing**, and **user testing**.

As development proceeds, work should proceed in updating the security plan as needed and developing supporting documents, which can include:

- Configuration management plan
- Continuous monitoring plan
- Security awareness, training, and education plan
- Incident response plan

functional testing
Security testing in which advertised security mechanisms of an information system are tested under operational conditions to determine if a given function works according to requirements.

penetration testing
Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, a system, or a network.

user testing
A phase of system development in which the software or system is tested in the "real world" by the intended audience. Also called **end-user testing**.

https://t.me/learningnets

Control Gates

The development/acquisition phase involves the following control gates:

- **Architecture/design review:** A review of the security architecture and design evaluates its integration with other systems and the overall enterprise architecture.
- **Performance review:** A review that evaluates whether the system meets the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use.
- **Functional test review:** A review that ensures that functional requirements are sufficiently detailed and are testable after deployment.
- **Risk management review:** A review of the risk management decisions made so far if there have been changes to the system or its security controls.
- **Mid-project status and financial review:** A review that determines if there have been changes in the planned level of effort and evaluates the effects on costs and benefits.

certification and accreditation (C&A)

A comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. *Accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Implementation/Assessment Phase

Figure 8.7 illustrates the relationship among four key security-related activities that comprise the implementation/assessment phase. In this phase, the organization configures and enables system security features, tests the functionality of these features, installs or implements the system, and obtains a formal authorization to operate the system.

Creating a Detailed Plan for C&A

An individual in the enterprise must be responsible for determining if the risks of operating the system and the cost of implementation, deployment, and operation are acceptable. This individual is referred to as the *authorizing official*. During this activity, the authorizing official works with the development team to discuss the forms of evidence needed for authorization and the procedures for submitting what is needed for **certification and accreditation (C&A)**. The expected output of this activity is an agreed work plan.

Integrating Security with Environments or Systems

The integration activity occurs at the point of deploying the system for operation. Security control settings are enabled, and other security features need to be integrated at this point. The output of this activity is a verified list of operational security controls integrated into the completed system documentation.

https://t.me/learningnets

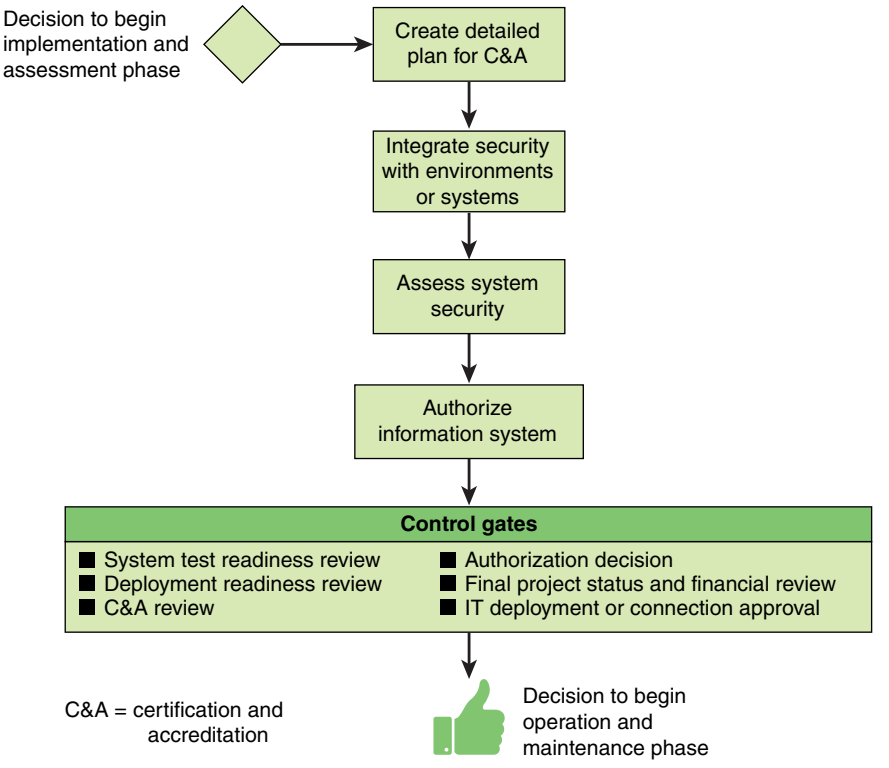


FIGURE 8.7 Security in the Implementation/Assessment Phase

Assessing System Security

The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk. This corresponds to step 4 in the NIST risk management framework defined in SP 800-37 (refer to Figures 6.1 and 6.2 in Chapter 6).

System security should be assessed for every security control that is part of the system design and implementation. NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, provides guidance on assessing each of the controls defined in SP 800-53. For example, Table 8.1 shows the security control definition of CP-3 (Contingency Training) in SP 800-53.

https://t.me/learningnets

TABLE 8.1 Security Control CP-3 in SP 800-53

CP-3 Contingency Training	
Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:	
CP-3(a)	Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;
CP-3(b)	When required by information system changes; and
CP-3(c)	[*Assignment: organization-defined frequency*] thereafter.
Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.	
Control Enhancements: (1) *CONTINGENCY TRAINING* | *SIMULATED EVENTS* Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. (2) *CONTINGENCY TRAINING* | *AUTOMATED TRAINING ENVIRONMENTS* Employ automated mechanisms to provide a more thorough and realistic contingency training environment.	
References: NIST Special Publication 800-50.	

Table 8.2 shows the assessment template for CP-3 that is defined in SP 800-53A. The shaded portion of Table 8.2 is not part of the template but provides an example of an assessment using the template.

TABLE 8.2 Example Assessment Findings for Control CP-3 Using Template from SP 800-53A

CP-3 Contingency Training		
ASSESSMENT OBJECTIVE: Determine if the organization provides contingency training to information system users consistent with assigned roles and responsibilities:		
CP-3(a)	CP-3(a)[1]	within the organization-defined time period of assuming a contingency role or responsibility; **(S)**

https://t.me/learningnets

CP-3 Contingency Training		
	CP-3(a)[2]	defines a time period within which contingency training is to be provided to information system users assuming a contingency role or responsibility; **(S)**
CP-3(b)	when required by information system changes; **(O)**	
CP-3(c)	CP-3(c)[1]	thereafter, in accordance with the organization-defined frequency; **(S)**
	CP-3(c)[2]	defines the frequency for contingency training. **(S)**
Potential Assessment Methods and Objects: Examine: [SELECT FROM: Contingency planning policy; procedures addressing contingency training; contingency plan; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities]. Test: [SELECT FROM: Organizational processes for contingency training].		
Comments and Recommendations: CP-3(b) is marked as other than satisfied because assessors could not find evidence that the organization provided contingency training to information system users consistent with their assigned roles and responsibilities when there were significant changes to the system.		

Note: Each determination statement contained within an assessment procedure executed by an assessor produces one of the following findings: *satisfied (S)* ; or *other than satisfied (O)*.

The expected output of this activity is a Security Accreditation Package, which includes the Security Assessment Report, the Plan of Action and Milestones (POA&M), and the updated System Security Plan. The POA&M is a document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist the organization in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Authorizing Information System

Authorization (also known as *security accreditation*) is granted by a senior official, based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to organization assets or operations (including mission, function, image, or reputation). Authorizing officials need to make risk decisions not only for the information system but also for the risk extended to the organization as a whole by placing the system into operation. The expected output of this activity is a documented security authorization decision.

https://t.me/learningnets

Control Gates

The implementation/assessment phase involves the following control gates:

- **System test readiness review:** A review to determine readiness to support system acceptance testing. It may include recommended changes to the test plan, test cases, test scripts, and requirement traceability matrixes.
- **Deployment readiness review:** A review to ensure that the system is ready to be integrated into the enterprise architecture.
- **Certification and accreditation (C&A) review:** A review to determine if the system is ready for certification and accreditation.
- **Authorization decision:** A decision to permit operation of the information system and to accept explicitly the residual risk to agency assets or operations.
- **Final project status and financial review:** A final review of the project and its financial impacts.
- **IT deployment or connection approval:** Approval to deploy the system and/or connect it to the rest of the enterprise architecture. The deployment or connection review is also referred to as an *operational readiness review* (*ORR*) and is intended to serve three primary purposes. First, the ORR provides a checkpoint to ensure that all of the processes needed to successfully deploy and maintain the system in production have been identified. Second, the ORR validates that the identified processes are completed. The final objective of the ORR is to achieve concurrence, via a "go/no-go" decision, that the system is ready for release into the production environment for sustained operations and maintenance support.

Operations and Maintenance Phase

Figure 8.8 illustrates the relationship among three key security-related activities that comprise the operations and maintenance phase. In this phase, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. During this phase, the organization should continuously monitor performance of the system to ensure that it is consistent with preestablished user and security requirements and to ensure that needed system modifications are incorporated.

Reviewing Operational Readiness

When a system transitions to an operational environment, unplanned modifications may be needed. If so, the ORR should be revisited to ensure that the system remains ready to be operational. Specifically, the system owner should evaluate the security implications of any system changes. These should be documented and updates to the security control suite made, if needed.

https://t.me/learningnets

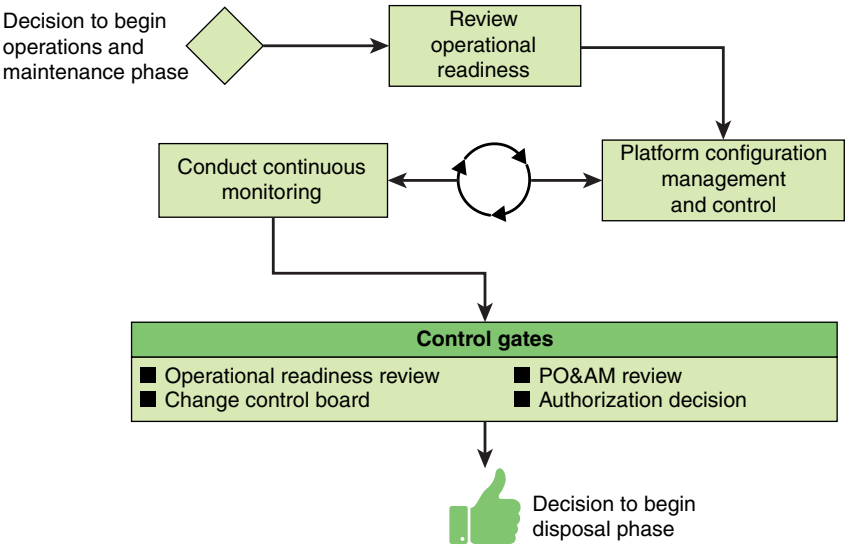


FIGURE 8.8 Security in the Operations and Maintenance Phase

Ensuring Configuration Management and Control

As discussed in Chapter 4, configuration management is the process of controlling modifications to a system's hardware, software, and documentation, which provides sufficient assurance that the system is protected against the introduction of improper modification before, doing, and after system implementation. Expected outputs include any decisions to make changes. Changes need to be done in a systematic matter using **change control**. In larger organizations, change decisions at this point are generally the responsibility of a **change control board (CCB)**.

change control
A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted, and that resources are used efficiently.

For configuration management (CM) and control, it is important to document the proposed or actual changes in the security plan of the system. Information systems are typically in a constant state of evolution, with upgrades to hardware, software, firmware, and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact of these changes on the security of a system is an essential part of continuous monitoring and key to avoiding a lapse in system security accreditation.

The expected output of this activity should include documentation of CCB decisions and security evaluations of documented system changes.

change control board (CCB)
A committee that makes decisions about whether proposed changes to a system should be implemented.

Conducting Monitoring Continuously

Coordinated with configuration management and control is continuous monitoring of the system. The ultimate objective of continuous monitoring is to determine whether the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the

https://t.me/learningnets

system operates. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits. Automation should be leveraged where possible to reduce the level of effort and ensure repeatability. Output should document the monitoring activity and any results.

Control Gates

The operations and maintenance phase involves the following control gates:

- **Operational readiness review:** The previously conducted operational readiness review should be revisited to ensure that changes are reviewed for risk potential.
- **Change control board:** The CCB reviews any proposed changes.
- **POA&M review:** This review revisits the POA&M to ensure that all action items are resolved.
- **Authorization decision:** The authorization decision needs to be revisited in response to changes.

Disposal Phase

Figure 8.9 illustrates the relationships among five key security-related activities that comprise the disposal phase. The disposal phase is the process of preserving (if applicable) and discarding system information, hardware, and software. During this phase, information, hardware, and software are moved to another system, archived, discarded, or destroyed. If performed improperly, the disposal phase can result in unauthorized disclosure of sensitive data.

Disposal, which is discussed in some detail in Chapter 7, involves the following key activities:

- **Create a disposal/transition plan:** This plan ensures that all stakeholders are aware of the future plan for the system and its information. The plan should document all the planned steps for disposal.
- **Ensure information protection:** Any information that is to be archived or otherwise retained must be accessible by appropriate hardware in the future. If the information is encrypted, appropriate key management functions must be invoked.
- **Sanitize media:** The procedures of SP 800-88, *Guidelines for Media Sanitization*, or a similar standards document should be followed to ensure thorough sanitization.
- **Dispose of hardware and software:** Hardware and software can be sold, given away, destroyed, or discarded, as provided by applicable law or regulation.
- **Close system:** The information system is formally shut down and disassembled at this point.

https://t.me/learningnets

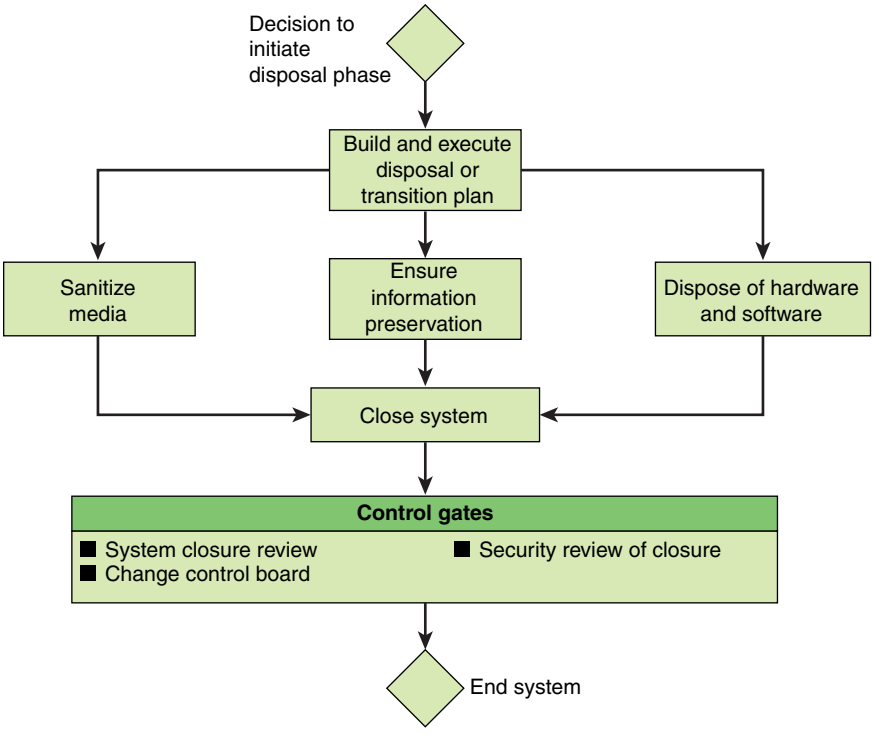


FIGURE 8.9 Security in the Disposal Phase

The disposal phase involves the following control gates:

- **System closure review:** The review should verify system closure, including final closure notification to the authorizing and certifying officials, configuration management system owner, information system security officer, and program manager.
- **Change control board:** The CCB needs to be formally notified.
- **Security review of closure:** Security documentation needs to be archived, as appropriate.

8.3 System Development Management

System develop management involves planning, delivering, operating, supporting, and evaluating the SDLC. Thus, system development management is an overall, high-level supervision of system development through all phases of the SDLC.

https://t.me/learningnets

The International Foundation for Information Technology [IFIT09] lists the following as functions of system development management:

- Identify and solicit demand for system development
- Create and set strategy for system development
- Perform research on or for system development
- Plan for the delivery of system development
- Identify requirements for system development
- Define and design system development
- Build or construct system development
- Control quality of or for system development
- Deliver system development (to meet identified demand or desire)
- Operate and support system development

In the following sections, we look at three aspects of system development management: system development methodology, system development environments, and quality assurance.

System Development Methodology

The foundation for effective system development management is the adoption of an SDLC methodology to be used on all system development projects. Any of the three methods discussed in Section 8.1, or some similar SDLC methodology, can serve this purpose. It is important to document the steps and deliverables of the SDLC and to assign roles and responsibilities.

The International Foundation for Information Technology [IFIT09] lists the following as principles or best practices for managing the SDLC that has been selected:

- **Ownership:** Assign accountability for system development management to key individuals, committees, or departments.
- **Inventory:** Maintain a central database of all items related to the management of system development, including requirements, deliverables, and the status of control gates.
- **Terminology:** Use standard terminology for the various aspects of system development.
- **Data centralization:** Data that are required by or useful for stakeholders involved in system development should be maintained in a central repository.

https://t.me/learningnets

- **Metrics:** There should be an agreed-upon set of performance metrics that can be defined, tracked, and analyzed to assess progress in system development.
- **Transparency:** Stakeholders should always strive to make any and all system development management data transparent to all other appropriate stakeholders, at a minimum, and often to the entire enterprises. The exception is when private user data must be protected. Many stakeholders often make the mistake of treating internal operational data as private or protected. This often creates a data silo and often leads to organizations revolving around such data silos.
- **Standards and best practices:** To the maximum extent possible, system development should be based on and follow industry standards and best practices.

System Development Environments

As systems evolve within and throughout the different phases of the SDLC as they are constructed, verified, and promoted from one working location to another. These IT industry calls these locations **environments**—typically virtual locations and are not necessarily physical locations, although they can be physically separated as well, if there is a requirement to do so.

environment

A particular configuration of hardware or software. A programming environment would include the compiler and associated development tools. The term environment is also used to express a type of configuration, such as a networking environment, database environment, transaction processing environment, batch environment, interactive environment, and so on.

Types of System Development Environments

The International Foundation for Information Technology [IFIT09] lists the following as distinct types of environments associated with system development:

- **Research:** This environment is used as an isolated sandbox for researching the viability of technologies and solutions, often implemented in the form of a proof of concept, a study, or an experiment.
- **Developer work space:** This environment accommodates the activities associated with the private or localized implementation that is performed by a single or individual resource, such as a software coder or an engineer, to provide an isolated working area that provides the flexibility to work freely without interference with or from other environments where other resources may be working.
- **Centralized build:** This environment accommodates the activities associated with centralized or merged builds. In this environment, the individual developer products are brought together to create a single, unified build.
- **Integration testing:** An isolated environment is used to test the integrations (that is, the data communications connections, channels, and exchanges) between the product, system, or software release being worked on and those of other products, systems, or instances of software that the release is intended to work with and communicate with during its operation in other downstream environments, such as production.

https://t.me/learningnets

- **User acceptance testing:** This environment enables human interaction with the system for the purpose of obtaining final approval and sign-off for the features and functions of the release.
- **Production:** This environment is the final targeted environment where a product, system, or software release operates for business use. This environment is deemed to be the most critical, as failures in this environment can potentially disturb or even shut down a line of business, depending on the importance of the product, system, or software being used by its end users.

Smaller projects or systems need not have all six of these environments.

Security Considerations for System Development Environments

System development presents two principal security requirements: security of the environment itself and security of the enterprise that exists outside the environment.

With respect to the security of the environment, the security objectives are twofold. First, the system owner should ensure that nothing outside the environment will contaminate or corrupt the environment in a manner that will prevent it from functioning as it is intended to function. This is essentially a denial-of-service issue in that an attacker may attempt to thwart the development of a new system by sabotaging the system development process. Second, the system owner needs to ensure that no malware or other function or feature is introduced into the system during development that may later be used maliciously in the operational environment.

With respect to the security of the enterprise, the system owner needs to ensure that nothing inside a specific environment escapes or is shared with resources or systems that operate in other environments without explicit knowledge and approval. Both of these aspects of environment security require that a number of key security areas be addressed, including the following [IFIT09]:

- **Environment access security:** This type of security focuses on determining what resources, systems, and roles have access to a specific environment, with the intent of minimizing outside influences and/or corruption.
- **Environment role and responsibility security:** This type of security focuses on ensuring that only the appropriately entitled roles can perform controlled and sanctioned work in an environment, which helps keep the right things in or out of it.
- **Environment data and information security:** This type of security focuses on ensuring that anything that has a level of confidentiality is protected and maintained, with the intent that data and information is shared only on an appropriate need-to-know basis.

https://t.me/learningnets

The SGP lists the following as some best practices that help provide the types of environment security previously listed:

- The various environments should be isolated from one another either physically or through secure virtual machine and virtual container technology.
- Application source code should be protected. This includes protection from malware and intruder attacks on the software.
- Information and application source code should be protected against unauthorized access or modification.
- Formal documented change management policies should be enforced.

Quality Assurance

Quality assurance deals with assessing compliance with requirements or standards. In developing products and services, quality assurance is any systematic process of checking to see whether a product or service being developed is meeting specified requirements. Many companies have a separate department devoted to quality assurance. A quality assurance system is said to increase customer confidence and a company's credibility, to improve work processes and efficiency, and to enable a company to better compete with others. Quality assurance systems emphasize catching defects before they get into the final product.

A person or group responsible for quality assurance in the SDLC should have a working knowledge of information security and how it can be used to enhance the quality of the program (for example, ensuring the integrity of computer-based information, the availability of services, and the confidentiality of customer information).

Important security-related quality assurance tasks for system development include:

- Assessing development risks (that is, those related to running a development project), which would typically include risks associated with business requirements, benefits, technology, technical performance, costing, and time scale
- Ensuring that security requirements have been clearly defined
- Confirming that security controls (for example, policies, methods, procedures, devices, or programmed mechanisms intended to protect the confidentiality, integrity, or availability of information) agreed-upon during the information risk assessment process have been developed and are working correctly
- Confirming that individuals responsible for developing, testing, and implementing systems under development are following the methodology

https://t.me/learningnets

8.4 System Development Best Practices

The SGP breaks down the best practices in the system development category into 2 areas and a number of topics and provides detailed checklists for each topic. These are the areas and topics:

- **System development management:** The objective of this area is to establish a structured system development methodology that applies to all types of business applications (including related systems and networks); is supported by specialized, segregated development environments; and involves a quality assurance process.
  - **System development methodology:** The objective of this topic is to ensure that systems (including those under development) meet business and information security requirements. The topic includes checklists of policies and procedures for meeting the objective.
  - **System development environments:** This topic discusses requirements and methods for isolating development and test environments from the live environments and each other.
  - **Quality assurance:** This topic lists elements and procedures needed for quality assurance.
- **System development life cycle:** The objective in this area is to define industry best practice for incorporating information security during each stage of the life cycle (refer to Figure 8.2). For each of the 10 stages, the SGP provides a checklist of considerations and actions to ensure that the system meets security requirements.

8.5 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

Agile software development
application life cycle management (ALM)
certification and accreditation (C&A)
change control
change control board (CCB)
DevOps
end-user testing
environment
functional testing
penetration testing
source code repository
system development life cycle (SDLC)
system owner
user testing
waterfall development

https://t.me/learningnets

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. What tasks are part of the initiation phase?
2. What are some of the testing types that are deployed during the development/acquisition phase?
3. What is the pilot run strategy in the changeover step of the implementation/assessment phase?
4. Explain DevOps as a method of software development and deployment.
5. What are typical stages in the life cycle of an application/system?
6. What are four phases of the DevOps reference architecture?
7. DevOps rests on two key foundations. Name them.
8. Explain the term *control gates* from SDLC point of view.
9. Enumerate key security considerations throughout the SDLC.
10. What are some of the control gates at the development/acquisition phase?
11. What are the key activities for the disposal phase?
12. According to the International Foundation for Information Technology, what are the best practices for managing the SDLC?
13. According to the International Foundation for Information Technology, what are some key environments associated with system development?

8.6 References

IFIT09: The International Foundation for Information Technology, *System Development Management*. 2009 https://www.if4it.com/SYNTHESIZED/DISCIPLINES/System_Development_Management_Home_Page.html.

MICR15: Microsoft, *Enterprise DevOps.* Microsoft white paper, 2015.

MINI14: Minick, E., Rezabek, J., & Ring, C., *Application Release and Deployment for Dummies.* Hoboken, NJ: Wiley, 2014.

SHAR15: Sharma, S., & Coyne, B., *DevOps for Dummies.* Hoboken, NJ: Wiley, 2015.

https://t.me/learningnets

Chapter 9

Business Application Management

The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.

—*On War*, Carl Von Clausewitz

Learning Objectives

After studying this chapter, you should be able to:

- Explain the three major components of application management.
- Discuss ways to incorporate security into business applications.
- Understand the specific security techniques for web applications.
- Understand the different challenges for end-user-developed applications compared to IT-developed applications.
- Describe a framework for managing security for end-user-developed applications.
- Present an overview of business application management best practices.

Business application management and security is a complex field. Applications encompass purpose-built applications developed in-house or by contractors, applications supplied by application and operating system vendors, and open source application software. Applications may operate on a variety of platforms, including workstations, PCs, mobile devices, and web based. They may also need to access and generate a wide variety of data files and databases.

This chapter begins with an overview of application management concepts. The following two sections address the quite different security challenges for IT-developed applications and applications developed by end users.

https://t.me/learningnets

9.1 Application Management Concepts

Application management (AM) provides a wide variety of application services, processes, and methodologies for maintaining, enhancing, and managing custom applications, packaged software applications, and network-delivered applications. It encompasses server-based, cloud-based, PC-based, and web-based applications used in the enterprise. AM is an enterprisewide IT governance approach geared toward providing an optimal application performance benchmark for organizations while incorporating business and IT segments, each with diverse AM objectives. Key AM stakeholders are:

application management (AM)
The process of managing the operation, maintenance, versioning, and upgrading of an application throughout its life cycle. AM includes best practices, techniques, and procedures that are essential to a deployed application's optimal operation, performance, and efficiency throughout the enterprise and back-end IT infrastructure.

- **Application owners:** This group consists of key business executive personnel who view AM in terms of business productivity, revenue, and control.
- **Application developers/managers:** This group consists of key IT enterprise personnel responsible for application development, deployment, and maintenance.
- **Application users:** For this group, AM is measured according to security, privacy, versioning, and overall control of application processes and modules.

AM processes include application life cycle management (ALM), application portfolio management (APFM), and application performance management (APM).

Application Life Cycle Management

Application life cycle management (ALM) is the process by which information technology and software development organizations create, deploy, and operate software over its full life cycle [GOUL15]. Thus, it is a form of system development life cycle (SDLC) management, and the considerations of Chapter 8, "System Development," apply to it. This section provides a brief overview.

application life cycle management (ALM)
The administration and control of an application from its inception to its demise. It embraces requirements management, system design, software development, and configuration management and implies an integrated set of tools for developing and controlling the project.

Figure 9.1 illustrates a typical ALM process that an enterprise may adopt. In includes the following phases:

- **Gather requirements:** IT works with the business units to identify the functional and business process requirements for the change or new application.
- **Design:** Based on the requirements, an application development team constructs a preliminary design of the software structure. The new software will impose resource requirements on the IT infrastructure, so IT analysts need to get involved at this stage. The IT analysts need to ensure that IT infrastructure resources either already exist or are acquired to meet the new resource requirements; this analysis typically involves the use of simulation tools and capacity prediction software. At this point, a **total cost of ownership (TCO)** study is performed to identify development and ongoing support costs.

https://t.me/learningnets

total cost of ownership (TCO)
A comprehensive analysis of a product or system that seeks to quantify the financial impact of deploying a product over its life cycle. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses, and the opportunity costs of downtime, training, and other productivity losses.

The appropriate business managers and perhaps higher management must then either approve the TCO commitment or work with IT analysts and planners to adjust the project cost to overall business unit plans.

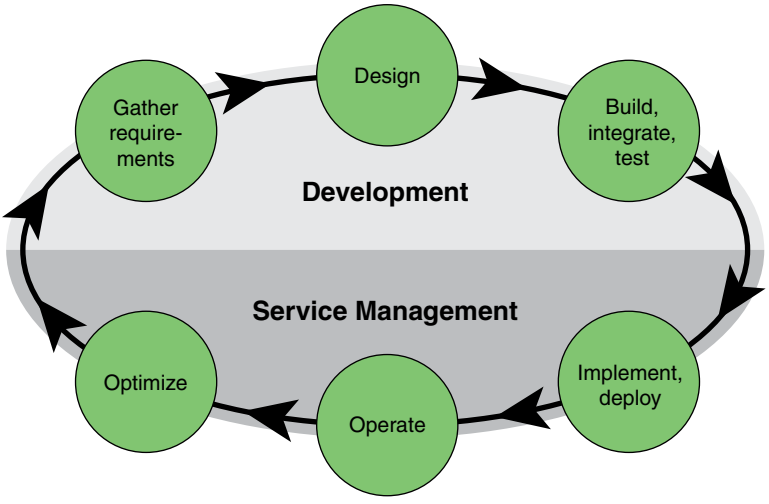


FIGURE 9.1 Application Life Cycle Management

- **Build, integrate, and test:** The application development team then develops and tests all the components and data flows. The team tests individual modules and the entire system to uncover any flaws. Testing includes the use of performance monitoring software and user interface testing. After final quality testing, management must sign off to move to implementation and deployment.
- **Implement and deploy:** With final approval, the application team proceeds to produce a finished implementation and load module into production libraries. The team provides user training and documentation so that the new application is used effectively and efficiently.
- **Operate:** During the operational phase of an application, IT staff monitor the application in the following areas:
  - Addressing changes in regulatory requirements
  - Fixing flaws uncovered in the application
  - Monitoring service levels (and addressing problems in missed service levels)
  - Measuring and reporting on application performance
- **Optimize:** Once there is a certain level of operational experience, IT analysts monitor and evaluate application use to determine if there are any opportunities for optimization. Areas of concern include performance, capacity utilization, end-user satisfaction and productivity.

https://t.me/learningnets

For applications that are not developed in-house, such as those provided by application and operating system vendors and open source applications, the emphasis of ALM is on the last three phases listed above.

Application Portfolio Management

IT management is often viewed as a constant battle to put out fires on a day-to-day basis. **Application portfolio management (APFM)** is meant to look beyond the day-to-day and evaluate an organization's IT infrastructure to decide when and where improvements should be made. To be effective, APFM must follow a structured and repeatable process for making evaluations and recommendation. When it is a standardized process, APFM can be scaled up to meet the needs of large organizations. The concepts of APFM have been integrated into business and enterprise software to help organizations automate these practices.

application portfolio management (APFM)

A technique that applies cost/benefit analysis and other business analytics to IT decision making. APFM looks at each program and piece of equipment as an asset within a company's overall portfolio and gives it a score based on factors such as age, importance, and number of users. Under APFM, further investment in upgrades or changes in the portfolio mix must be justified by projected returns and other measurable factors.

APFM involves a number of considerations. The entire collection of applications running on various platforms within the organization or available via organization accounts in the cloud or on the web comprises the application portfolio. Various business units and departments may have authority to acquire or develop applications in-house. This can lead to duplication, security risks, and lack of integration of applications with enterprise strategic objectives. APFM is concerned with taking an overall look at the entire application portfolio in order to make better decisions about when to eliminate, upgrade, replace, or consolidate applications.

The concept of the application portfolio was first described and illustrated using a strategic matrix that demonstrated the importance of IT to the enterprise in McFarlan's article "The Information Archipelago—Plotting a Course" [MCFA83]. Figure 9.2 shows the use of such a matrix to illustrate the general strategy for assessing applications.

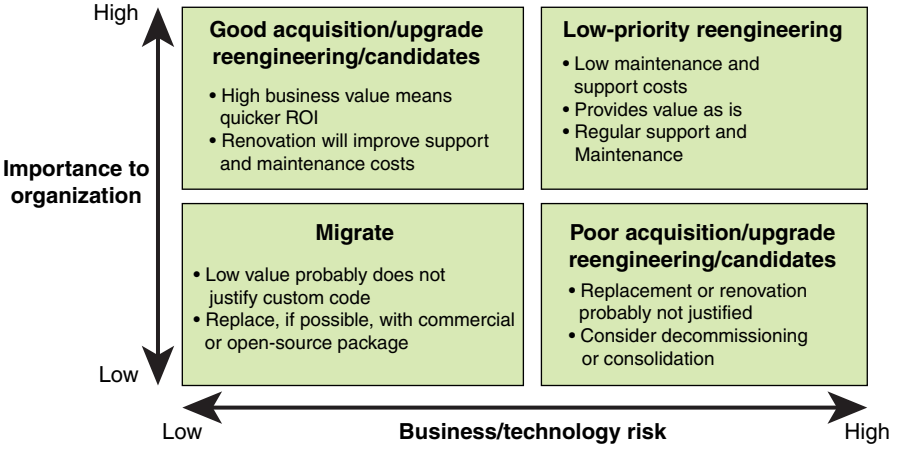


FIGURE 9.2 Strategic Matrix for Application Portfolio Management

https://t.me/learningnets

The matrix accounts for two dimensions in managing an application portfolio, and the key characteristics are defined in Table 9.1.

TABLE 9.1 Dimensions of an Application Portfolio Management Matrix

Value of the Application to the Enterprise	
Typical Characteristics of a High-Value Application	**Typical Characteristics of a Low-Value Application**
■ Meets present service delivery needs, business process **reengineering** initiatives, and information access ■ Meets anticipated needs for new services ■ Protective of individual privacy and data confidentiality	■ Creates inefficient and less effective service delivery processes ■ Places constraint on implementation of new services, expanded benefits, and/or efficient business processes ■ Places individual privacy and data confidentiality at risk
Cost/Risk of the Application to the Enterprise	
Typical Characteristics of a High-Cost/High-Risk Application	**Typical Characteristics of a Low-Cost/Low-Risk Application**
■ Is expensive to operate or maintain ■ Offers no or decreasing vendor support for major components ■ Provides insufficient or decreasing availability of staff support ■ Does not allow enhancements for new business requirements ■ Contributes to inefficient IT resource utilization ■ Provides inadequate data access and quality ■ Provides vulnerable security ■ Makes recoverability difficult or suspect	■ Is cost-effective to operate and maintain ■ Comes with adequate vendor support for major components ■ Provides adequate availability of staff support ■ Allows enhancements for new business requirements ■ Offers efficient IT resource utilization ■ Provides adequate data access and quality ■ Provides adequate security protection ■ Is resilient to human-induced or natural disasters

reengineering

Using information technology to improve performance and cut costs. The main premise of reengineering is to examine the goals of an organization and to redesign work and business processes from the ground up rather than simply automate existing tasks and functions.

The classification of each existing or contemplated application into one of the four quadrants is a useful aid in portfolio management. It supports prioritization and establishing a time frame for action.

Table 9.2 lists some best practices for application portfolio management recommended in the U.S. Government Accountability Office report *Portfolio Management Approach Needed to Improve Major Acquisition Outcomes* [GAO12].

https://t.me/learningnets

TABLE 9.2 Key Portfolio Management Practices

Outcome	Best Practices
Clearly define and empower leadership	■ Those responsible for product investment decisions and oversight should be clearly identified and held accountable for outcomes. ■ Portfolio managers should be empowered to make decisions about the best way to invest resources. ■ Portfolio managers should be supported with cross-functional teams composed of representatives from key functional areas.
Establish standard assessment criteria and demonstrate comprehensive knowledge of the portfolio	■ Specific criteria should be used to ensure transparency and assessment criteria and demonstrate comprehensive knowledge of the portfolio comparability across alternatives. ■ Investments should be ranked and selected using a disciplined process to assess the costs, benefits, and risks of alternative products. ■ Knowledge should encompass the entire portfolio, including needs, gaps, and how to best handle the gaps.
Prioritize investments by integrating the requirements, acquisition, and budget processes	■ Requirements, acquisition, and budget processes should be connected to promote stability and accountability. ■ Organizations should use an integrated approach to prioritize needs and allocate resources so they can avoid pursuing more products than they can afford and optimize return on investment. ■ Resource allocation across the portfolio should align with strategic goals/objectives and investment review policy should use long-range planning.
Continually make go/no-go decisions to rebalance the portfolio	■ Program requirements should be reviewed annually to make recommendations on proposed changes/descoping options. ■ As potential new products are identified, portfolios should be rebalanced based on those that add the most value. ■ If project estimates breach established thresholds, the product should be immediately reassessed within the context of the portfolio to determine whether it is still relevant and affordable. ■ Agencies should use information gathered from post-implementation reviews of investments, as well as information learned from other organizations, to fine-tune the investment process and the portfolios to shape strategic outcomes.

Application Performance Management

Application performance management (APM) is concerned with how well an application meets its intended purpose and performs as expected. The Gartner report

https://t.me/learningnets

application performance management (APM)
The practice within systems management that targets managing and tracking the availability and efficiency of software applications. APM involves translating IT metrics into business terminology. It examines the workflow and the associated IT tools that are deployed to analyze, identify, and report application performance concerns to make sure the expectations of businesses and end users are met.

Magic Quadrant for Application Performance Monitoring [KOWA12] defines five steps that comprise an effective APM strategy (see Figure 9.3):

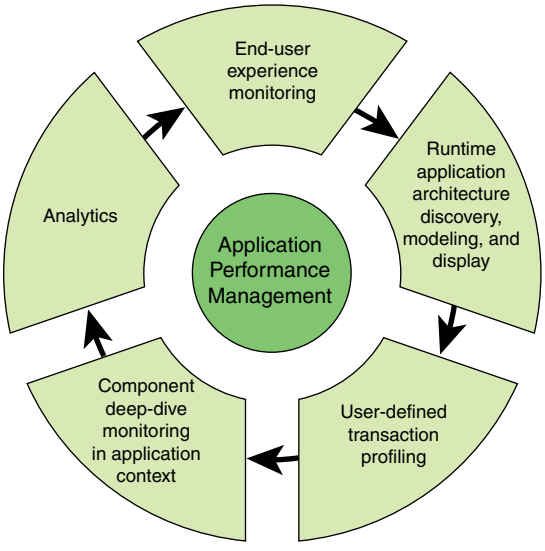


FIGURE 9.3 Application Performance Management Steps

1. **End user experience monitoring:** The first step is to capture data on how end-to-end performance impacts the user and identify any problem. This step is the most important. It doesn't matter if the internal metrics that are used seem to show that an application is delivering good performance. If the application seems slow or unresponsive to the user, then there is a performance problem.
2. **Runtime application architecture discovery, modeling, and display:** The second step is to study the software and hardware components involved in application execution, as well as their communication paths, to establish the potential scope of the problem. This step is designed to discover the specific components that contribute to an application's performance. This may include both hardware and software components. For example, a database server may be broken down into components such as processor, memory, disk, query execution time, and so forth.
3. **User-defined transaction profiling:** The third step involves examining user-defined transactions as they move across the paths defined in step 2 to identify the source of the problem. Here, the concern is not so much with the total transaction time as with what portions of the application are spending time

https://t.me/learningnets

processing the transaction. The objective is to determine what portions or layers of an application consume the most time. If the end user response time is above a given threshold, this information indicates where optimization efforts should be concentrated.

4. **Component deep-dive monitoring in an application context:** The fourth step is an in-depth monitoring of the resources consumed by, and events occurring within, the components discovered in step 2.
5. **Analytics:** The final step involves the use of analytics—including technologies such as behavior learning engines—to crunch the data generated in the first four steps, discover meaningful and actionable patterns, pinpoint the root cause of the problem, and ultimately anticipate future issues that may impact the end user.

9.2 Corporate Business Application Security

Application security overlaps with many of the topics covered in other chapters but needs to be considered as a separate security concern as well. The aim of web application security is to identify the following:

application security
The use of software, hardware, and procedural solutions to protect applications from external threats. This includes adding features or functionality to application software to prevent a range of different threats. It also includes security features outside the application, such as firewalls, antivirus software, and access control methods.

- Critical assets of the organization
- Genuine users who may access the data
- The level of access provided to each user
- Various vulnerabilities that may exist in the application
- Data criticality and risk analysis on data exposure
- Appropriate remediation measures

The following sections examine some of the main aspects of application security relevant to applications that are hosted by or used by enterprises.

Business Application Register

As part of application portfolio management, there should be an inventory, or register, of all applications, with details concerning the application, including security-related aspects. Table 9.3 lists information that should be included in the register.

https://t.me/learningnets

TABLE 9.3 Information to Be Included in a Business Application Register

Category	Information
Type	■ Developed in-house, **commercial-off-the-shelf (COTS) software**, cloud-based software, mobile-based software, end user-developed software
Operational	■ Business purpose ■ Business processes supported by the application ■ Relative importance to the organization (for example, critical, important, nonessential) ■ Owner
Users	■ Type and number of users ■ Type and volume of connections
Access security	■ Method of user authentication ■ Network security barriers (for example, firewall, IPsec)
Type of data accessed	■ Personally identifiable information ■ Sensitive information (requires strong confidentiality) ■ Requires strong availability ■ Requires strong integrity
Technical	■ Application version ■ Supplier and licensing requirements ■ Technical support contact

commercial-off-the-shelf (COTS) software

Software that is commercially available, leased, licensed, or sold to the general public and that requires no special modification or maintenance over the life cycle of the product to meet the needs of the procuring agency.

Business Application Protection

As with other business assets, sound security architecture principles should be applied to business applications. The considerations are somewhat different for two categories: internally developed applications and externally-developed applications.

Internal Application Security

For any application that is developed within the organization, it is essential to incorporate security into all stages of the SDLC. This task is illustrated and covered in detail in Section 8.2 in Chapter 8.

Whether an application is developed in-house or acquired, a number of measures should be in force, including the following:

- Document security requirements.
- Develop standardized procedures for evaluating application security products and services.
- Enforce compliance with government and industry standards and regulations.
- Formulate a policy that defines an acceptable security level for each application.

https://t.me/learningnets

- Develop a policy for pre-deployment application testing and validation.
- Develop a policy for post-deployment application monitoring.
- Construct a policy for documentation of application code review.
- Enforce routine patching/maintenance cycles.

The measures listed above are concerned with what might be referred to as *internal* application security. Here the concern is the development and validation of application-level security controls provided by the application itself. This would include measures such as encryption, key management, public-key certificate handling, and access methods built into the application.

External Application Security

When it comes to application security, internal security is important, but so is the external environment, including the host operating system or virtual operating system, the hardware platform, and network connections. Other chapters in this book address the security controls that are provided by the overall enterprise system environment, which include the following:

- Protection against unauthorized access using access control measures at the operating system level
- Enforcement of data confidentiality by using least privilege, separation of duties, firewalls, and measures to prevent disclosure of the internal working of applications
- Enforcement of virtual platform security
- Assurance that database and file system access by the application have adequate security controls
- Encryption of network traffic using Transport Layer Security (TLS) or Internet Protocol Security (IPsec)

Browser-Based Application Protection

As enterprises move applications online, both for internal use and for external users, such as customers and vendors, web application security becomes an increasing concern. The following sections examine some security considerations for web applications.

https://t.me/learningnets

Web Application Security Risks



Open Web Application Security Project https://www.owasp.org

Web applications, because of their nature, are at risk from a wide variety of threats. The applications are hosted on a server available over the Internet or other networks, usually using Hypertext Transfer Protocol Secure (HTTPS). Any given application may exhibit internal weaknesses, weaknesses associated with the server operating systems, or connection-based weaknesses. A useful guide to the most serious risks is the top 10 list of risks maintained by the Open Web Application Security Project (OWASP). Table 9.4 shows the 2017 version of this list [OWAS17], which was compiled with the input of a wide range of organizations.

TABLE 9.4 OWASP Top 10 Application Security Risks (2017)

Risk	Description
Injection	Injection flaws, such as Structured Query Language (SQL), operating system, and Lightweight Directory Access Protocol (LDAP) injection, occur when untrusted data are sent to an interpreter as part of a command or query. The hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
Sensitive data exposure	Many web applications and application programming interfaces (APIs) do not properly protect sensitive data. Attackers may steal or modify such weakly protected data. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
XML external entity	This type of attack parses Extensible Markup Language (XML) input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server-side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.
Broken access control	With this type of attack, restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as gaining access other users' accounts, viewing sensitive files, modifying other users' data, and changing access rights.

https://t.me/learningnets

Risk	Description
Security misconfiguration	Security misconfiguration is the most common issue in data, due in part to manual or ad hoc configuration, insecure default configurations, open S3 buckets, misconfigured HTTP headers, error messages containing sensitive information, and failure to patching or upgrade systems, frameworks, dependencies, and components in a timely fashion.
Cross-site scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or when an application updates an existing web page with user-supplied data using a browser API that can create JavaScript. XSS allows attackers to execute in the victim's browser scripts that can hijack user sessions, deface websites, or redirect users to malicious sites.
Insecure deserialization	Insecure deserialization flaws occur when an application receives hostile serialized objects, which can lead to remote code execution. Even if deserialization flaws do not result in remote code execution, serialized objects can be replayed, tampered with, or deleted to spoof users, conduct injection attacks, and elevate privileges.
Using components with known vulnerabilities	Components such as libraries, frameworks, and other software modules run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
Insufficient logging and monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show that the time to detect a breach is over 200 days, and such breaches are typically detected by external parties rather than internal processes or monitoring.

Web Application Firewall

The most important tool in countering web application threats is a **web application firewall (WAF)**, a firewall that monitors, filters, or blocks data packets as they travel to and from a web application. Running as a network appliance, server plug-in, or cloud service, a WAF inspects each packet and uses a rule base to analyze Layer 7 web application logic and filter out potentially harmful traffic. Firewalls are examined in detail in Chapter 12, "Networks and Communication."

A WAF is placed logically between an application and users such that all traffic to and from the application goes through the WAF. Figure 9.4 depicts this logical context.

https://t.me/learningnets

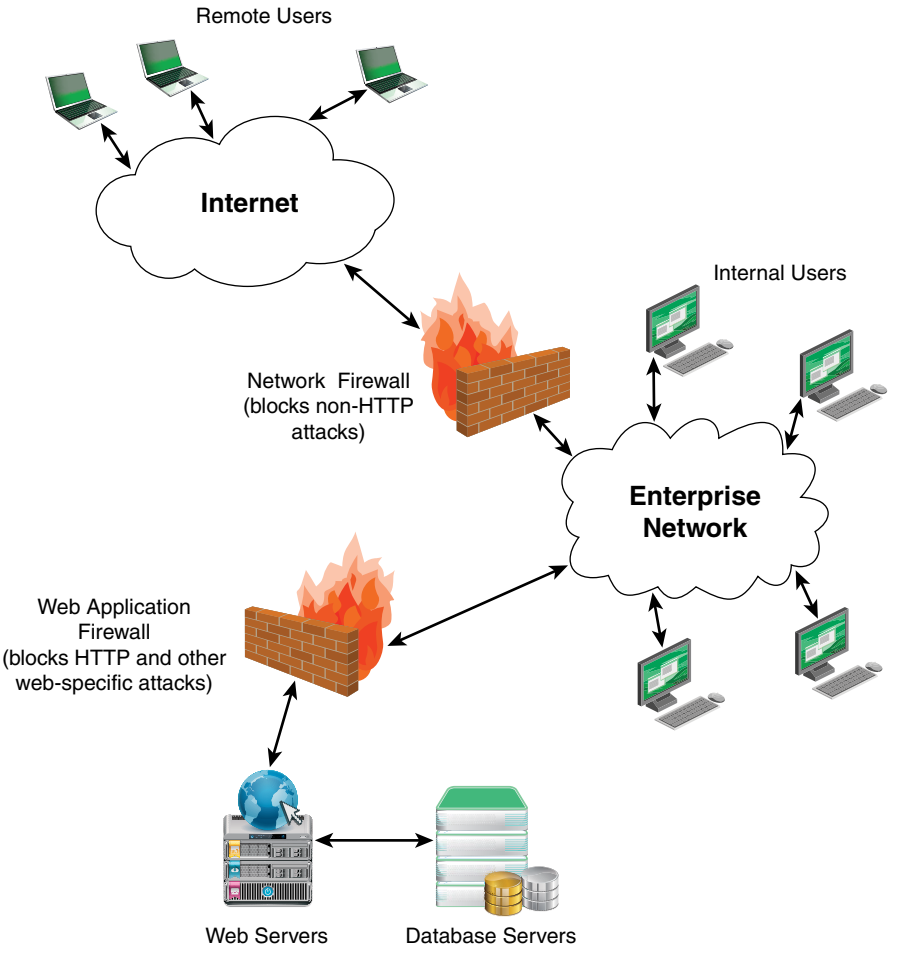


FIGURE 9.4 Context for a Web Application Firewall

There are a number of hosting options for WAFs, including the following:

- **Network-based:** A network-based firewall is a hardware firewall incorporated with a router at the edge of an enterprise network, acting as a filter to all traffic to and from network devices, including web-based application servers. Because there may be a variety of web applications on a number of servers, this approach can be complex to maintain. In addition, a network-based firewall may not be placed so as to catch internal traffic.
- **Local hardware:** A local hardware firewall is placed between the application server and its network connection or connections. This type of firewall is much simpler than a network-based firewall because it only has to have logic for filtering traffic specific to the local server.

https://t.me/learningnets

- **Local software:** A local software firewall is built on the server host operating system or virtual machine operating system. This approach can be as effective as a local hardware firewall and is easier to configure and modify.

An example of a WAF is ModSecurity, an open source software WAF. It is cross-platform capable (Apache, IIS, and Nginx) and enables web application defenders to gain visibility into HTTP(S) traffic and provides a language and API to implement monitoring, logging, and access control. Key features of ModSecurity include:



ModSecurity http://modsecurity.org

- **Real-time application security monitoring and access control:** All HTTP traffic in both directions passes through ModSecurity, where it can be inspected and filtered. ModSecurity also has a persistent storage mechanism, which enables tracking of events over time to perform event correlation.
- **Virtual patching:** This is the ability to apply web application patching without making changes directly to the application. Virtual patching is applicable to applications that use any communication protocol, but it is particularly useful with HTTP because the traffic can generally be well understood by an intermediary device.
- **Full HTTP traffic logging:** Web servers traditionally do very little when it comes to logging for security purposes. ModSecurity gives you the ability to log events, including raw transaction data, which is essential for forensics. In addition, the system manager gets to choose which transactions are logged, which parts of a transaction are logged, and which parts are sanitized.
- **Web application hardening:** This is a method of attack surface reduction in which the system manager selectively narrows down the HTTP features that will be accepted (for example, request methods, request headers, and content types).

reverse proxy

A server that accepts requests from the Internet and makes requests to a server or application sitting behind it. Unlike a forward-proxy, the client may not be aware that it is communicating with a reverse proxy; a reverse proxy receives requests as if it were the origin server for the target resource.

ModSecurity can be deployed as an embedded software package on the same server as the web applications. It can also be deployed on a separate server that can protect a number of web servers from one central location. This approach is a type of **reverse proxy** server. It provides complete isolation and dedicated resources to the firewall function.

Other Browser-Based Application Protection Measures

Beyond the use of a WAF, there are some other specific security measures that should be considered, including the following:

- Provide confidentiality and integrity protection for configuration files and other information specific to the application by isolating the files from other programs on the server and restricting file access.
- Website content should similarly have confidentiality and integrity protections.
- Oversight in the form of regular content review is needed to ensure that the content is not inappropriate and is accurate.

https://t.me/learningnets

Web Application Security Policy

According to a number of global threat reports, including the European Union Agency for Network and Information Security (ENISA') *ENISA Threat Landscape Report 2016* [ENIS17] and the Verizon *2018 Data Breach Investigations Report* [VERI18], web application vulnerabilities account for the largest portion of attack vectors after malware. Veracode's *State of Software Security 2017* [VERA17] found that existing security measures intended to protect web applications routinely fail, with more than half of web applications affected by misconfigured secure communications or other security defenses and 25% of web applications running on web servers containing at least one high-severity vulnerability.

It is therefore important for an organization to have and enforce a web application security policy. The policy template provided by the SANS Institute is good model to use. The following sidebar shows a key excerpt of this template.

Web Application Security Policy

Policy

4.1 Web applications are subject to security assessments based on the following criteria:

- **a)** New or Major Application Release – Will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- **b)** Third Party or Acquired Web Application – Will be subject to full assessment after which it will be bound to policy requirements.
- **c)** Point Releases – Will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- **d)** Patch Releases – Will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- **e)** Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- **a)** High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.

https://t.me/learningnets

b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

9.3 End User-Developed Applications (EUDAs)

In many enterprises, some business processes are supported by user-developed applications referred to as EUDAs that are outside the formal systems supported by the IT organization. These applications are typically developed by technically savvy users within the business function. They sometimes are created by a group within the department that is responsible for reporting or metrics calculations. These applications can go beyond reporting and actually augment or replace functionality contained in the formal system. Usually, these applications are not directly programmed in a programming language but use a common tool, such as Microsoft Excel, to create spreadsheet programs or a database management system, such as Microsoft Access, to create database functions. These applications may be hosted on shared drives, workgroup folders, or internal websites, or they may simply be emailed around. Some of these applications can evolve to be considered mission critical by the business unit.

https://t.me/learningnets

Examples of activities by end user programmers include:

- Using spreadsheets for accounting
- Using MatLab for analysis
- Creating a web page
- Recording macros in Word
- Automating office tasks
- Creating business software (SAP programming)
- Dong scientific research and calculation
- Authoring educational software
- Creating email filters

Benefits of EUDAs

Benefit of EUDAs include the following:

- **Convenience and ease of use:** EUDAs can be developed easily and quickly by non-IT staff. Business users frequently become frustrated with the amount of time taken by the IT department to service their requests. They therefore often resort to developing their own solutions, using applications such as Microsoft Excel to meet their reporting needs. EUDAs allow businesses and users to quickly deploy solutions in response to shifting market and economic conditions, industry changes, or evolving regulations.
- **Powerful tools and technology-aware end users:** End-user tools offer rich functionality, including the ability to connect to corporate data sources. As a result, technology-savvy users can perform powerful data processing from their desktops. This can help plug functionality gaps for business systems.
- **Demand for information:** Traditionally, managers were often constrained by standard reports in IT systems that failed to meet all management information and reporting requirements. The lack of flexibility in these systems and increasing demand for different views of the data have resulted in an increase in the level of end-user computing in organizations.

Risks of EUDAs

User-developed and user-controlled applications are generally not subject to the same development, monitoring, and reporting rigor and control as traditional applications. In addition, management often lacks visibility into exactly how pervasive EUDAs

https://t.me/learningnets

have become throughout the enterprise. This leads to a number of disadvantages and risks related to EUDAs, including the following:

- **Errors:** Errors can occur at data entry, in formulas, in application logic, or with links to other applications or data sources. Without a sound SDLC discipline, such errors are bound to occur. This could result in poor decision making or inaccurate financial reporting.
- **Poor version and change control:** EUDAs can be more difficult to control than traditional IT-developed applications. Even where change control policies exist, they can be difficult to enforce.
- **Poor documentation:** Files that have not been properly documented may be used incorrectly after a change in ownership of the EUDA, or they may just be used improperly in general. Again, this can lead to unintended and undetected errors.
- **Lack of security:** Unsecured files may be easily traded among users, which introduces the risk of changes to portions of data that should remain constant. This can lead to increased errors or might allow sensitive and confidential information to be seen by unauthorized users. An EUDA could possibly be used to perpetrate fraud or hide losses.
- **Lack of an audit trail:** The ability to audit and control changes to key data is essential both for internal governance and for compliance with external regulation. For critical applications, managing this risk effectively is crucial, and in many instances, it requires monitoring and controlling changes at a detailed level.
- **Regulatory and compliance violations:** A host of regulations deal with security and privacy for which an enterprise is responsible.
- **Risk of the unknown:** The greatest operational risk with EUDA usage is in not knowing the size of the potential problem. The use of EUDAs is so widespread that it may be extremely difficult to assess just how many EUDAs exist, how many are used in critical business applications, how they are linked together, and where data is fed into or extracted from other IT applications. To quantify this risk, it is necessary to carry out a full inventory of EUDA usage and a detailed risk assessment of all business-critical spreadsheets.
- **Opportunity cost:** Scarce resources (money or employee time) may be wasted on developing these applications.

EUDA Security Framework

To deal with the many risks associated with the use of EUDAs, enterprises need a comprehensive security framework that formalizes procedures for managing EUDAs and clarifies organizational policy. One such framework, consisting of four elements,

https://t.me/learningnets

is described in Juergens et al.'s article "End-User Computing: Solving the Problem" [JUER13] and illustrated in Figure 9.5.

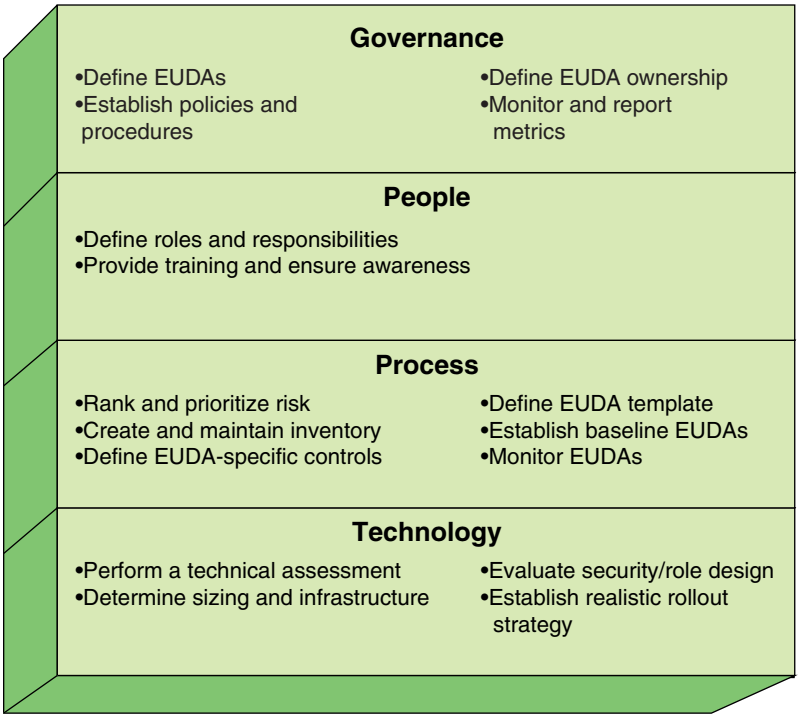


FIGURE 9.5 EUDA Security Framework

Governance

The first set of considerations is in the area of governance. Senior executives must define what constitutes an EUDA. This involves distinguishing EUDAs from IT-developed and supported applications and specifying which types of EUDAs should be placed under management control.

Next, an EUDA policy document is needed to provide a consistent framework for EUDA control. Be sure the policy defines criteria, inventory standards, risk ranking, and control requirements. Define a set of identification, tracking, and reporting metrics associated with all phases of the EUDA program.

Regardless of which individuals develop an EUDA, the organization should assign ownership responsibility to ensure that the policy document is enforced. This could either be done through an enterprise project management office or by assigning an owner within each business unit, or some combination or variation.

https://t.me/learningnets

People

Proper management and control of EUDAs requires identifying the key stakeholders in the EUDA management program. Once the key stakeholders are identified, the next step is to establish the roles and responsibilities. Stakeholder roles include the program sponsor, central program group, steering committee, business unit representatives, EUDA users, and internal auditors.

The organization should develop a training program to target each of the stakeholder groups. Examples of the training include EUDA policy implementation, EUDA risks and controls steps, and tool training involving end users and administrators.

Process

Management's top concerns with respect to EUDAs are the potential risks of any given application. The risk assessment concepts described in Chapter 3, "Information Risk Assessment," should be applied. Some framework for risk assessment is needed, and it could as simple as the risk analysis worksheet described in the beginning of Section 3.2. For each EUDA, the EUDA owner can apply the risk model to determine which EUDAs should be placed under formal management control.

As with IT-developed applications, as part of application portfolio management, there should be an inventory or register of all EUDAs that are under management control, with details concerning the application, including security-related aspects. Table 9.3 can be used for EUDAs.

For each EUDA, based on its risk and impact assessment, the EUDA owner should select the appropriate controls, which should include the following:

- **Version control:** Helps ensure that the latest and approved version of an EUDA is used throughout the organization
- **Change control:** Helps ensure that the changes to EUDAs are appropriately tracked and reviewed
- **Data integrity control:** Helps ensure data integrity
- **Access control:** Helps ensure that only authorized users can access EUDAs and in what manner (for example, view, change, delete)
- **Availability control:** Helps ensure that EUDAs are available in the event of disaster, accidental deletion, and so on

To assist in the monitoring and control of EUDAs, management should define a set of templates, one for each type of EUDA. The template is a guide to the creation and documentation of EUDAs that promotes consistency throughout the organization.

https://t.me/learningnets

Once an EUDA has been created, the EUDA owner should be required to establish a baseline, which involves validating the structures, formulas, calculations, inputs, and outputs of the EUDA. Once the controls and baseline of an EUDA are established, the owner is responsible for periodic testing to monitor the effectiveness of the controls and to ensure that user groups continue to adhere to defined controls.

Technology

In the area of technology, the organization should perform an assessment to see what sorts of tools and enablers exist or should be acquired to support the development of EUDAs. Specific EUDA management software tools can be deployed, or native functionality (such as Microsoft SharePoint) can be used, with various degrees of functionality available.

Next, the organization needs to assess the impact of new EUDAs in terms of sizing and infrastructure needs. For example, if network file shares will be used to secure EUDAs, does the current server population have the estimated capacity to accept the additional load? Other considerations may impact this as well. For example, will one enterprise server be used, or will each global region have a separate server for managing EUDAs?

The organization should develop technical solutions to enforce access control. The access control involves in the first instance which users have access to use a given EUDA. At a more detailed level, a detailed security role design can define different levels of access for different roles.

Finally, management needs to develop a schedule for moving EUDAs into the management framework and providing oversight for the rollout of new EUDAs as they are approved.

9.4 Business Application Management Best Practices

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) breaks down the best practices in the Business Application Management category into two areas and eight topics and provides detailed checklists for each topic. The areas and topics are:

- **Corporate business applications:** The objective of this area is to incorporate security controls into business applications (including specialized controls for web browser–based applications) to protect the confidentiality and integrity of information when it is input to, processed by, and output from these applications.

https://t.me/learningnets

- **Business application register:** This topic summarizes the information, including security-related information, that should be maintained in an inventory or a register of all business applications.
- **Business application protection:** Summarizes basic security principles and applies them to business applications.
- **Browser-based application protection:** Covers measures that should be taken to secure enterprise applications that are available via a web browser.
- **Information validation:** Summarizes basic security principles to protect confidentiality and integrity and applies them to information when it is input into, processed by, and output from business applications.

- **End user-developed applications (EUDAs):** The objective of this area is to develop critical EUDAs, such as spreadsheets, in accordance with an approved development methodology, which covers validating input, implementing access control, restricting user access to powerful functionality, and recording them in an inventory:
  - **EUDA inventory:** Lists the types of information that should be included in an EUDA inventory.
  - **Protection of spreadsheets:** Discusses the types of access controls that should be used and the user training that should be provided.
  - **Protection of databases:** Discusses the types of access controls that should be used and the user training that should be provided.
  - **EUDA development:** Lists considerations in controlling and managing EUDA development.

9.5 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

application life cycle management (ALM)
application management (AM)
application performance management (APM)
application portfolio management (APFM)
application security
commercial-off-the-shelf (COTS)
end-user-developed application (EUDA)
reengineering
reverse proxy
total cost of ownership (TCO)
web application firewall (WAF)

https://t.me/learningnets

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. What does the term *application management* mean?
2. Who are the key stakeholders of application management?
3. Explain the typical stages of application life cycle management.
4. What does TCO stand for, and what does it mean?
5. According to Gartner, what are the steps of an effective APM strategy?
6. What does COTS stand for, and what does it mean? Give some examples of COTS.
7. What is ModSecurity? Highlight some of its salient features.
8. List some of the benefits of EUDAs.
9. What are the main risks related to EUDAs?
10. How many elements are there in the security framework for EUDAs?

9.6 References

ENIS18: European Union Agency for Network and Information Security. *ENISA Threat Landscape Report 2017.* January 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

GAO12: U.S. Government Accountability Office, *Portfolio Management Approach Needed to Improve Major Acquisition Outcomes.* GAO-12-918, September 2012.

GOUL15: Gould, L., "Introducing Application Lifecycle Management." *Automotive Design and Production Magazine*, November 2015.

JUER13: Juergens, M., Donohue, T., & Smith, C., "End-User Computing: Solving the Problem." *CompAct*, April 2013. https://www.soa.org/News-and-Publications/Newsletters/Compact/2013/april/End-User-Computing-Solving-the-Problem.aspx.

KOWA12: Kowall, J., & Cappelli, W., *Magic Quadrant for Application Performance Monitoring.* Gartner Report, 2013. https://www.gartner.com/doc/2125315/magic-quadrant-application-performance-monitoring.

https://t.me/learningnets

MCFA83: McFarlan, F., "The Information Archipelago—Plotting a Course." *Harvard Business Review*, January 1983.

OWAS17: The OWASP Foundation. OWASP Top 10 2017: The Ten Most Critical Web Application Security Risks. 2017 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

VERA17: Veracode, *State of Software Security 2017.* 2017 https://info.veracode.com/report-state-of-software-security.html.

VERI18: Verizon, *2017 Data Breach Investigations Report.* 2018 https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

https://t.me/learningnets

Chapter 10

System Access

"Badges? We ain't got no badges! We don't need no badges! I don't have to show you any stinking badges!!"

—The Treasure of the Sierra Madre, 1948

Learning Objectives

After studying this chapter, you should be able to:

- Discuss the three general means of authenticating a user's identity.
- Explain the mechanism by which hashed passwords are used for user authentication.
- Present an overview of password-based user authentication.
- Present an overview of hardware token-based user authentication.
- Present an overview of biometric user authentication.
- Summarize some of the key security issues for user authentication.
- Present an overview of system access best practices.

This chapter presents an overview of system access concepts, including a discussion of authorization. The chapter focuses on user authentication and its many aspects and security issues.

10.1 System Access Concepts

System access is the capability that restricts access to business applications, mobile devices, systems, and networks to authorized individuals for specific business purposes. System access comprises three distinct functions:

- **Authentication:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. This function is often referred to as *user authentication*, to distinguish it from message authentication or data authentication.

https://t.me/learningnets

- **Authorization:** In the context of system access, authorization is the granting of access or other rights to a user, program, or process to access system resources. Authorization defines what an individual or program can do after successful authentication.
- **Access control:** The process of granting or denying specific requests for accessing and using information and related information processing services and for entering specific physical facilities. Access control ensures that access to assets is authorized and restricted based on business and security requirements.

The three functions are shown in Figure 10.1.

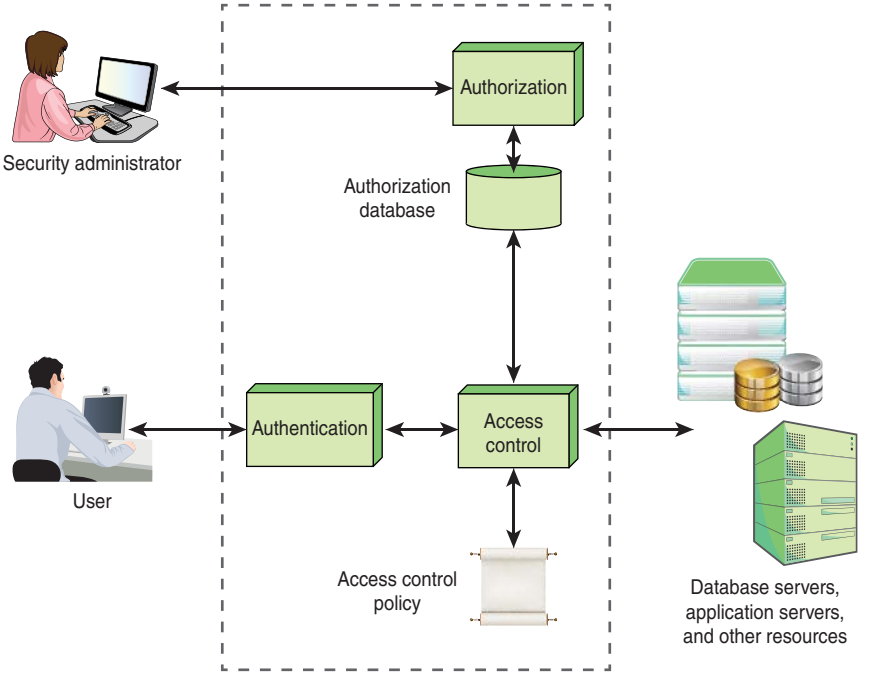


FIGURE 10.1 System Access Functions

All the elements depicted within the dashed lines in Figure 10.1 are referred to as *access control*. To make it clear that all the listed functions are related, the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) uses the term *system access* to refer to the service provided by authorization, authentication, and access control working together.

https://t.me/learningnets

System access is concerned with denying access to unauthorized users and limiting the activities of legitimate users to only those actions they are authorized to perform on system resources. The access control function mediates attempted access to an object in the system by a user or a program executing on behalf of that user. The authentication function establishes the identity of the user. The authorization function maintains an authorization database that defines the access privileges for each user. The access control function consults the authorization database and uses an access control policy that specifies how a user's privileges are to be mapped into allowable actions for specific data items or other resources.

The remainder of this section discusses authorization. Authentication is covered in Sections 10.2 through 10.7. A discussion of access control is deferred until Chapter 14, "Technical Security Management."

Authorization

A designated security administrator is responsible for creating and maintaining the authorization database. The administrator sets these authorizations on the basis of the security policy of the organization and the roles and responsibilities of individual employees. The process for authorizing users should include the following:

- Associating access privileges with uniquely defined individuals, for example by using unique identifiers, such as user IDs.
- Maintaining a central record of access rights granted to a user ID to access information systems and services.
- Obtaining authorization from the owner of the information system or service for the use of the information system or service. Separate approval for access rights from management may also be appropriate.
- Applying the principle of least privilege to give each person the minimum access necessary to do his or her job.
- Assigning individual access privileges for resources based on information security levels and classification of information.
- Specifying the networks and networked services to be accessed, such as files and databases.
- Defining requirements for expiration of privileged access rights.
- Ensuring that identifiers are not reused. This means deleting authorizations associated with a user ID when the individual assigned that user ID changes roles or leaves the organization.

https://t.me/learningnets

In addition to taking the normal security protections used to protect databases, review the authorization database on a regular basis to ensure that access privileges remain appropriate and that obsolete authorizations have been deleted.

10.2 User Authentication

User authentication is one of the most complex and challenging security functions. There are a wide variety of methods of authentication, with associated threats, risks, and countermeasures. This section provides an overview of them. The following three sections look at the three general authentication factors: password, hardware token, and biometric. Then Section 10.6 discusses risk assessment.

In most computer security contexts, user authentication is a fundamental building block and the primary line of defense. User authentication is the basis for most types of access control and for user accountability. User authentication encompasses two functions:

- **Identification step:** This step involves presenting an identifier to the security system. (Assign identifiers carefully because authenticated identities are the basis for other security services, such as access control service.)
- **Verification step:** This step involves presenting or generating authentication information that corroborates the binding between the entity and the identifier.

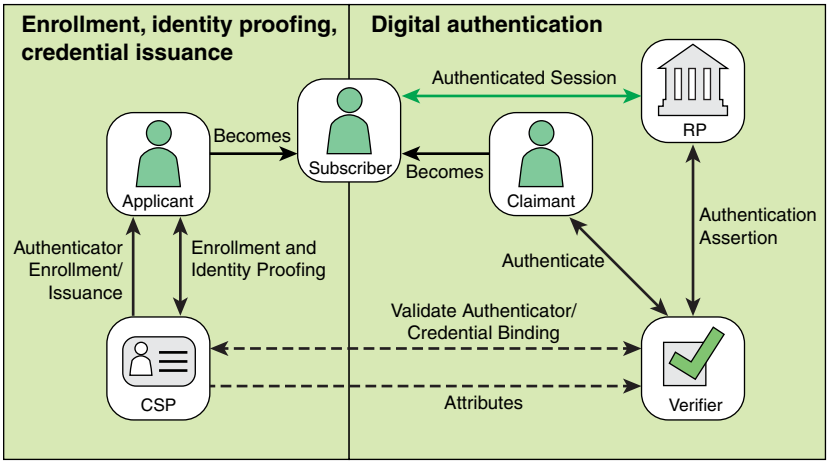
For example, say that user Alice Toklas has the user ID ABTOKLAS. This information needs to be stored on any server or computer system that Alice wishes to use and could be known to system administrators and other users. A typical item of authentication information associated with this user ID is a password, which is kept secret (known only to Alice and to the system). If no one is able to obtain or guess Alice's password, then the combination of Alice's user ID and password enables administrators to set up Alice's access permissions and audit her activity. Because Alice's ID is not secret, system users can send her e-mail, but because her password is secret, no one can pretend to be Alice.

In essence, *identification* is the means by which a user provides a claimed identity to the system, and *authentication* is the means of establishing the validity of the claim.

A Model for Electronic User Authentication

National Institute of Standards and Technology (NIST) SP 800-63, *Digital Identity Guidelines*, defines a general model for user authentication that involves a number of entities and procedures, as shown in Figure 10.2.

https://t.me/learningnets



CSP = credential service provider
RP = relying party

FIGURE 10.2 The NIST 800-63 Digital Identity Model

Three concepts are important in understanding this model:

- **Digital identity:** The digital identity is the unique representation of a subject engaged in an online transaction. The representation consists of an attribute or set of attributes that uniquely describe a subject within a given context of a digital service but does not necessarily uniquely identify the subject in all contexts.
- **Identity proofing:** This process establishes that a subject is who he or she claims to be to a stated level of certitude. This process involves collecting, validating, and verifying information about a person.
- **Digital authentication:** This process involves determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as the subject that previously accessed the service.

Six entities are defined in Figure 10.2:

- **Credential service provider (CSP):** A trusted entity that issues or registers subscriber authenticators. For this purpose, the CSP establishes a digital credential for each subscriber and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.

https://t.me/learningnets

- **Verifier:** An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators, using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.
- **Relying party (RP):** An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.
- **Applicant:** A subject undergoing the processes of enrollment and identity proofing.
- **Claimant:** A subject whose identity is to be verified using one or more authentication protocols.
- **Subscriber:** A party who has received a credential or authenticator from a CSP.

The left-hand portion of Figure 10.2 illustrates the process whereby an applicant is enrolled in the system for purposes of accessing certain services and resources. First, the applicant presents to the CSP evidence of possession of the attributes to be associated with this digital identity. Upon successful proofing by the CSP, the applicant becomes a subscriber. Then, depending on the details of the overall authentication system, the CSP issues some sort of electronic credential to the subscriber. The **credential** is a data structure that authoritatively binds an identity and additional attributes to one or more authenticators possessed by a subscriber and is verified when presented to the verifier in an authentication transaction. The authenticator is either an encryption key or an encrypted password that identifies the subscriber. The authenticator is issued by the CSP, generated directly by the subscriber, or provided by a third party. The authenticator and credential may be used in subsequent authentication events. The details of identity proofing are discussed in Chapter 14.

Once a user is registered as a subscriber, the authentication process takes place between the subscriber and one or more systems that perform authentication (refer to the right-hand portion of Figure 10.2). The party to be authenticated is called a *claimant*, and the party verifying that identity is called a *verifier*. When a claimant successfully demonstrates possession and control of an authenticator to a verifier through an authentication protocol, the verifier verifies that the claimant is the subscriber named in the corresponding credential. The verifier passes on an assertion about the identity of the subscriber to the RP. That assertion includes identity information about a subscriber, such as the subscriber's name, an identifier assigned at registration, or some other subscriber attribute that was verified in the registration process. The RP uses the authenticated information provided by the verifier to make access control or authorization decisions. (Access control is discussed further in Chapter 14.)

https://t.me/learningnets

In some cases, the verifier interacts with the CSP to access the credential that binds the subscriber's identity and authenticator and to optionally obtain claimant attributes. In other cases, the verifier does not need to communicate in real time with the CSP to complete the authentication activity (as with some uses of digital certificates). Therefore, the dashed line between the verifier and the CSP in Figure 10.2 represents a logical link between the two entities.

An implemented system for authentication differs from—and is usually more complex than—this simplified model, but this model illustrates the key roles and functions needed for a secure authentication system.

Means of Authentication

authentication factor

A method of authentication, based on either something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints or other forms of biometrics).

There are three general means of authenticating a user's identity—called **authentication factors**—which are used alone or in combination:

- **Knowledge factor (something the individual knows):** The user must demonstrate knowledge of secret information. Knowledge factors, routinely used in single-layer authentication processes, can come in the form of passwords, passphrases, personal identification numbers (PINs), or answers to secret questions.
- **Possession factor (something the individual possesses):** The authorized user must present a physical entity to connect to the client computer or portal. This type of authenticator used to be referred to as a token, but that term is now deprecated. The term hardware token is a preferable alternative. Possession factors fall into two categories:
  - **Connected hardware tokens:** Items that connect to a computer logically (e.g., via wireless) or physically in order to authenticate identity. Items such as smart cards, wireless tags, and USB tokens are common connected tokens used to serve as possession factors.
  - **Disconnected hardware tokens:** Items that do not directly connect to the client computer but instead require input from the individual attempting to sign in. Typically, a disconnected hardware token device uses a built-in screen to display authentication data that are then utilized by the user to sign in when prompted.
- **Inherence factor (something the individual is or does):** These are characteristics, called biometrics, that are unique or almost unique to the individual. These include static biometrics, such as fingerprint, retina, and face; and dynamic biometrics, such as voice, handwriting, and typing rhythm.

https://t.me/learningnets

The specific items used during authentication, such as a password or hardware token, are referred to as **authenticators**.

authenticator
The means used to confirm the identity of a user, process, or device (for example, user password, hardware token). An authentication factor is based on the use of a particular type of authenticator.

All these methods, properly implemented and used, provide secure user authentication. However, each method has problems, as shown in Table 10.1. An adversary may be able to guess or steal a password. Similarly, an adversary may be able to forge or steal a card. A user may forget a password or lose a card. A user might share a password or card with a colleague. Furthermore, there is significant administrative overhead for managing password and card information on systems and securing such information on systems. With respect to biometric authenticators, there are a variety of problems, including dealing with false positives and false negatives, user acceptance, cost, security of the sensor itself, and convenience.

TABLE 10.1 Authentication Factors

Factor	Examples	Properties
Knowledge	User ID Password PIN	Can be shared Many passwords are easy to guess Can be forgotten
Possession	Smart card Electronic badge Electronic key	Can be shared Can be duplicated (cloned) Can be lost or stolen
Inherence	Fingerprint Face Iris Voice print	Not possible to share False positives and false negatives possible Forging difficult

Sections 10.3 through 10.5 examine password, hardware token, and biometric approaches.

Multifactor Authentication

Multifactor authentication refers to the use of more than one of the authentication means in the preceding list (see Figure 10.3). The strength of an authentication system is largely determined by the number of factors incorporated by the system. A system that requires two factors is generally stronger than a system requiring a single factor, assuming that the individual factors are reasonably strong. A three-factor system is generally stronger than a two-factor system, although at some point diminishing returns sets in.

https://t.me/learningnets

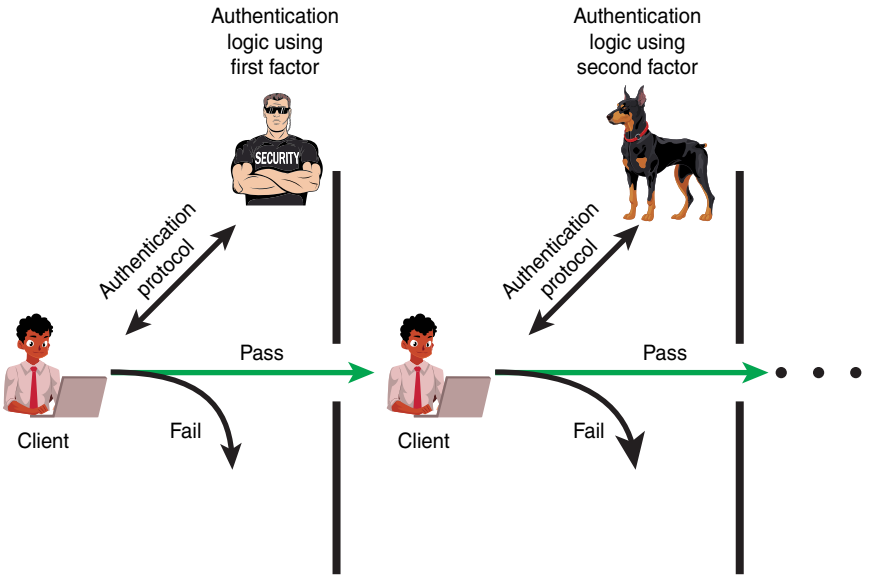


FIGURE 10.3 Multifactor Authentication

10.3 Password-Based Authentication

What you know is a widely used line of defense against intruders is a password system. Virtually all multiuser systems, network-based servers, web-based ecommerce sites, and other similar services require that a user provide not only a name or identifier (ID) but also a password. The system compares the password to a previously stored password for that user ID, maintained in a system password file. The password serves to authenticate the ID of the individual logging on to the system. In turn, the ID provides security in the following ways:

- The ID determines whether the user is authorized to gain access to a system. In some systems, only those who already have an ID filed on the system are allowed to gain access.
- The ID determines the privileges accorded to the user. A few users may have supervisory or "superuser" status that enables them to read files and perform functions that are especially protected by the operating system. Some systems have guest or anonymous accounts, and users of these accounts have more limited privileges than others.
- The ID is used in what is referred to as *discretionary access control*. For example, by listing the IDs of the other users, a user may grant permission to them to read files owned by that user.

https://t.me/learningnets

The Vulnerability of Passwords

Typically, a server that uses password-based authentication maintains a password file indexed by user ID. When logging on or making an access request, a user presents both his or her ID and password. The server looks up the password for that ID in the password file to determine if there is a match. One security technique that is typically used is to store not the user's password but a one-way hash function of the password, as described subsequently.

Attack strategies and countermeasures are identified as follows:

- **Offline dictionary attack:** Typically, strong access controls are used to protect a system's password file. However, determined hackers frequently bypass such controls and gain access to password files. An attacker who obtains a system password file compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker gains access by using that ID/password combination. Countermeasures include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords in the event that the password file is compromised.
- **Specific account attack:** In this type of attack, an attacker targets a specific account and submits password guesses until the correct password is discovered. The standard countermeasure is an account lockout mechanism, which locks out access to the account after a number of failed login attempts. Typical practice is no more than five access attempts.
- **Popular password attack:** A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess. Countermeasures include policies to inhibit the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns.
- **Password guessing against a single user:** An attacker may attempt to gain knowledge about an account holder and system password policies and uses that knowledge to guess the user's password. Countermeasures include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, minimum length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed.
- **Workstation hijacking:** In this type of attack, an attacker waits until a logged-in workstation is physically unattended. The standard countermeasure is automatically logging out the workstation after a period of inactivity. Intrusion detection schemes are used to detect changes in user behavior.

https://t.me/learningnets

- **Exploiting user mistakes:** If the system assigns a password, then the user is more likely to write it down because it is difficult to remember. This situation creates the potential for an adversary to read the written password. A user may intentionally share a password to enable a colleague to share files, for example. Also, attackers are frequently successful in obtaining passwords by using social engineering tactics that trick the user or an account manager into revealing a password. Many computer systems are shipped with preconfigured passwords for system administrators. Unless these preconfigured passwords are changed, they are easily guessed. Countermeasures include user training, intrusion detection, and simpler passwords combined with another authentication mechanism.
- **Exploiting multiple password use:** Attacks become much more effective or damaging if different network devices share the same or a similar password for a given user. Countermeasures include a policy that forbids using the same or similar password on particular network devices.
- **Electronic monitoring:** If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping. Simple encryption does not fix this problem because the encrypted password is, in effect, the password and can be observed and reused by an adversary.

Despite the many security vulnerabilities of passwords, they remain the most commonly used user authentication technique, and this is unlikely to change in the foreseeable future [HERL12]. Among the reasons for the persistent popularity of passwords are the following:

- Techniques that utilize client-side hardware, such as fingerprint scanners and smart card readers, require the implementation of the appropriate user authentication software to exploit this hardware on both the client and server systems. Until there is widespread acceptance on one side, there is reluctance to implement on the other side, and the result is a who-goes-first stalemate.
- Physical tokens, such as smart cards, are expensive and/or inconvenient to carry around, especially if multiple tokens are needed.
- Schemes that rely on a single sign-on to multiple services, using one of the non-password techniques described in this chapter, create a single point of security risk.
- Automated password managers that relieve users of the burden of knowing and entering passwords have poor support for roaming and synchronization across multiple client platforms, and their usability had not been adequately researched.

https://t.me/learningnets

Thus, it is worth your while to study the use of passwords for user authentication in some detail.

The Use of Hashed Passwords

A widely used password security technique is the use of hashed passwords and a salt value. This scheme is found on virtually all UNIX variants as well as on a number of other operating systems. This technique is shown in Figure 10.4a. To load a new password into the system, the user selects or is assigned a password. The system combines the password with a fixed-length salt value. In older implementations, this value was related to the time at which the password was assigned to the user. Newer implementations use a pseudorandom or random number. The password and salt serve as inputs to a hashing algorithm to produce a fixed-length hash code. The hash algorithm is designed to be slow to execute in order to thwart attacks. The hashed password is then stored, together with a plaintext copy of the salt, in the password file for the corresponding user ID. The hashed password method has been shown to be secure against a variety of cryptanalytic attacks [WAGN00].

When a user attempts to log on to a UNIX system, the user provides an ID and a password, as shown in Figure 10.4b. The operating system uses the ID to index into the password file and retrieve the plaintext salt and the hashed password. The salt and user-supplied password are used as input to the hash algorithm. If the result matches the stored value, the password is accepted.

The salt serves three purposes:

- It prevents duplicate passwords from being visible in the password file. Even if two users choose the same password, those passwords are assigned different salt values. Hence, the hashed passwords of the two users differ.
- It greatly increases the difficulty of offline dictionary attacks. For a salt of length b bits, the number of possible passwords is increased by a factor of 2^b, increasing the difficulty of guessing a password in a dictionary attack.
- It becomes nearly impossible to find out whether a person with passwords on two or more systems used the same password on all of them.

To see the second point, consider the way that an offline dictionary attack works. The attacker obtains a copy of the password file. Suppose that the salt is not used. The attacker's goal is to guess a single password. To that end, the attacker submits a large number of likely passwords to the hashing function. If any of the guesses matches one of the hashes in the file, the attacker has found a password that is in the file. But faced with the UNIX scheme, the attacker must take each guess and submit it to the hash function once for each salt value in the dictionary file, greatly increasing the number of guesses that must be checked.

https://t.me/learningnets

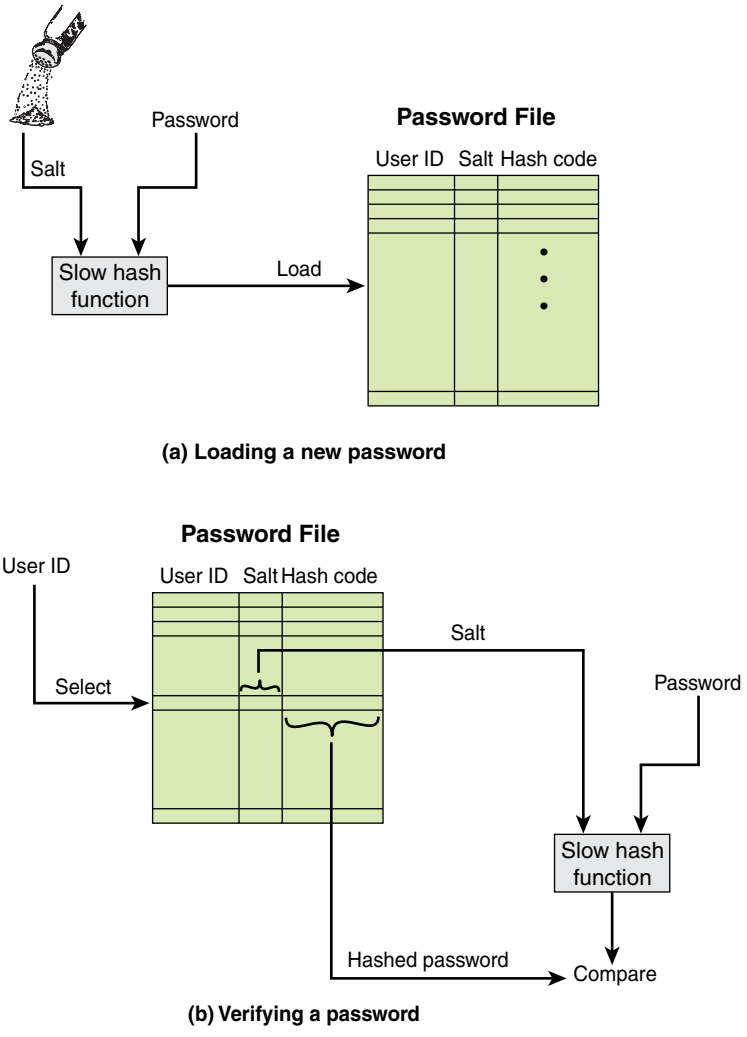


FIGURE 10.4 UNIX Password Scheme

There are two threats to the UNIX password scheme. First, a user can gain access on a machine by using a guest account or by some other means and then run a password guessing program, called a password cracker, on that machine. The attacker is able to check many thousands of possible passwords with little resource consumption. In addition, if an attacker is able to obtain a copy of the password file, then a cracker program can be run on another machine at leisure. This enables the attacker to run through millions of possible passwords in a reasonable period.

https://t.me/learningnets

Password Cracking of User-Chosen Passwords

Password cracking is the process of recovering secret passwords stored in a computer system or transmitted over a network. This section looks at some approaches to password cracking that have been used for many years but are still in some cases effective, as well as more modern, sophisticated approaches.

Traditional Approaches

The traditional approach to password cracking is to develop a large dictionary of possible passwords and to try each of them against the password file. This means that each password must be hashed using each available salt value and then compared to stored hash values. If no match is found, the cracking program tries variations on all the words in its dictionary of likely passwords. Such variations include backward spelling of words, additional numbers or special characters, a sequence of identical characters

An alternative is to trade off space for time by precomputing potential hash values. In this approach, the attacker generates a large dictionary of possible passwords. For each password, the attacker generates the hash values associated with each possible salt value. The result is a mammoth table of hash values known as a *rainbow table*. For example, Oechslin's article "Making a Faster Cryptanalytic Time-Memory Trade-Off" [OECH03] showed that using 1.4 GB of data, he could crack 99.9% of all alphanumeric Windows password hashes in 13.8 seconds. This approach is countered by using a sufficiently large salt value and a sufficiently large hash length. Both FreeBSD and OpenBSD, which are open source versions of UNIX, use this approach, and so should be secure from this attack for the foreseeable future.

To counter the use of large salt values and hash lengths, password crackers exploit the fact that some people choose easily guessable passwords. A particular problem is that users, when permitted to choose their own password, tend to choose short ones. Bonneau's "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords" [BONN12] summarizes the results of a number of studies over the past few years involving over 40 million hacked passwords, as well as their own analysis of almost 70 million anonymized passwords of Yahoo users. They found a tendency to use six to eight characters and no or few nonalphanumeric characters in passwords.

Bonneau's analysis of the 70 million passwords estimates that passwords provide fewer than 10 bits of security against an online, trawling attack and only about 20 bits of security against an optimal offline dictionary attack [BONN12]. In other words, an attacker who manages 10 guesses per account, typically within the realm of rate-limiting mechanisms, compromises around 1% of accounts, just as the attacker would do against random 10-bit strings. Against an optimal attacker performing an

https://t.me/learningnets

unrestricted brute-force attack and wanting to break half of all available accounts, passwords appear to be roughly equivalent to 20-bit random strings. Therefore, using an offline search enables an adversary to break a large number of accounts, even if a significant amount of iterated hashing is used.

Password length is only part of the problem. Many people, when permitted to choose their own password, pick a password that is guessable, such as their own name, their street name, a common dictionary word, and so forth. This makes the job of password cracking straightforward. The cracker simply has to test the password file against lists of likely passwords. Because many people use guessable passwords, such a strategy succeeds on virtually all systems.

Attacks that use a combination of brute-force and dictionary techniques have become common. A notable example of this dual approach is John the Ripper, an open-source password cracker [OPEN15].

Modern Approaches

Sadly, password cracking has not lessened in the past 25 years or so. Users are doing a better job of selecting passwords, and organizations are doing a better job of forcing users to pick stronger passwords (a concept known as a *complex password policy* and discussed later in this section). However, password-cracking techniques have improved to keep pace. The improvements are of two kinds. First, the processing capacity available for password cracking has increased dramatically. Now used increasingly for computing, graphics processors allow password-cracking programs to work thousands of times faster than they did just a decade ago on similarly priced PCs that used traditional CPUs alone. A PC running a single AMD Radeon HD7970 GPU, for instance, can try on average an 8.2×10^9 password combinations each second, depending on the algorithm used to scramble them [GOOD12]. Only a decade ago, such speeds were possible only when using pricey supercomputers.

To develop techniques that are more efficient and effective than simple dictionary and brute-force attacks, researchers and hackers have studied the structure of passwords. To do this, analysts need a large pool of real-word passwords to study, which they now have. The first big breakthrough came in late 2009, when a Structured Query Language (SQL) injection attack against online games service RockYou.com exposed 32 million plaintext passwords used by its members to log in to their accounts [TIMM10]. Since then, numerous sets of leaked password files have become available for analysis.

Using large data sets of leaked passwords as training data, Weir et al.'s "Password Cracking Using Probabilistic Context-Free Grammars" [WEIR09] reports on the development of a probabilistic context-free grammar for password cracking. In this approach, guesses are ordered according to their likelihood, based on the frequency of their character-class structures in the training data, and based on the frequency of

https://t.me/learningnets

their digit and symbol substrings. This approach is shown to be efficient in password cracking [KELL12, ZHAN10].

Mazurek et al., in their article "Measuring Password Guessability for an Entire University" [MAZU13], report on an analysis of the passwords used by more than 25,000 students at a research university with a complex password policy. The analysts used the password-cracking approach introduced in "Password Cracking Using Probabilistic Context-Free Grammars" [WEIR09]. They used a database consisting of a collection of leaked password files, including the RockYou file. With this technique, more than 10% of the passwords were recovered after only 10^{10} guesses; after 10^{13} guesses, almost 40% of the passwords were recovered.

Password File Access Control

One way to thwart a password attack is to deny the attacker access to the password file. If the hashed password portion of the file is accessible only by a privileged user, then the attacker cannot read it without already knowing the password of a privileged user. Often, the hashed passwords are kept in a separate file from the user IDs, referred to as a *shadow password file*. Special attention is paid to making the shadow password file protected from unauthorized access. Although password file protection is certainly worthwhile, there remain vulnerabilities, including the following:

- Many systems, including most UNIX systems, are susceptible to unanticipated break-ins. A hacker may be able to exploit a software vulnerability in the operating system to bypass the access control system long enough to extract the password file. Alternatively, the hacker may find a weakness in the file system or database management system that allows access to the file.
- An accident of protection might render the password file readable, thus compromising all the accounts.
- Some of the users may have accounts on other machines in other protection domains, and they may use the same password of all of them. Thus, if the passwords can be read by anyone on one machine, a machine in another location might be compromised.
- A lack of or weakness in physical security may provide opportunities for a hacker. Sometimes there is a backup to the password file on an emergency repair disk or archival disk. Access to this backup enables the attacker to read the password file. Alternatively, a user can boot from a disk running another operating system such as Linux and access the file from that operating system.
- Instead of capturing the system password file, another approach to collecting user IDs and passwords is through sniffing network traffic.

https://t.me/learningnets

Thus, a password protection policy must complement access control measures with techniques to force users to select passwords that are difficult to guess.

Password Selection

When not constrained, many users choose a password that is too short or too easy to guess. At the other extreme, if users are assigned passwords consisting of eight randomly selected printable characters, password cracking is effectively impossible. But it is almost as impossible for most users to remember such passwords. Fortunately, even if you limit the password universe to strings of characters that are reasonably memorable, the size of the universe is still too large to permit practical cracking. The goal, then, is to eliminate guessable passwords while allowing the user to select a password that is memorable.

User-Selected Passwords

In many contexts, it is appropriate for the user to select the password to be used. In this case, the CSP or similar entity generally provides enforceable guidelines indicating what passwords are acceptable. The most notable form of these is composition rules, which require the user to choose passwords constructed using a mix of character types, such as at least one digit, uppercase letter, and symbol. However, an exhaustive study reported in Weir et al.'s "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords." [WEIR10] revealed that the benefit of such rules is not nearly as significant as initially thought, and the negative impact on usability and memorability is severe. Thus, users are allowed to create passwords that are easily memorized, provided that they are resistant to dictionary and brute-force guessing attacks.

The other common guideline concerns password length. A number of studies, such as Kelley et al.'s "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. [KELL12] and Komanduri's "Of Passwords and People: Measuring the Effect of Password-Composition Policies" [KOMA11], have shown that password length is a primary determinant of password strength against both brute-force and dictionary attacks. Accordingly, users are encouraged to make passwords as long as they want, within reason. For example, allowing a user to choose a string of easy-to-remember words with spaces in between—such as "turtle box super liquor"—instead of imposing something like X30UnMx$# provides a combination of security and usability.

Based on this and similar research reports, NIST significantly revised its guidelines for user-selected passwords for the 2017 edition of SP 800-63, which says that passwords must be at least 8 characters in length and may be up to 64 characters in length.

https://t.me/learningnets

Regulating Password Selection

When processing requests to establish and change memorized secrets, the CSP (or verifier) needs to take measures to ensure strong password selection. SP 800-63B, *Digital Identity Guidelines—Authentication and Lifecycle Management*, recommends the following requirements:

- The CSP should provide feedback during or just after the password is entered in the form of a strength metric, which is either strength labels (for example, weak, fair, strong) or a thermometer-type scale. Different meters rely on client-side heuristics, server-side Markov models, or artificial neural networks to gauge password strength [HABI17].
- Reject any password that is on a **blacklist** maintained by the CSP. SP 800-63B suggests that the blacklist should include the following:
  - Passwords obtained from previous breach corpuses. A good source is Burnett's list of 10 million compromised passwords [BURN15].
  - Dictionary words.
  - Repetitive or sequential characters (for example aaaaaa, 1234abcd).
  - Context-specific words, such as the name of the service, the username, and derivatives thereof.
- Following rejection of a blacklisted password, the CSP should reject any trivial modification of the rejected password.
- Verifiers shall not prompt subscribers to use specific types of information (for example, "What was the name of your first pet?") when choosing memorized secrets.
- Verifiers shall not permit the subscriber to store a hint that is accessible to an unauthenticated claimant.

blacklist
A list of discrete entities, such as hosts, applications, or passwords, that have been previously determined to be associated with malicious activity and are not approved for use within an organization and/or information system.

List of 10 Million Compromised Passwords

https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495

System-Selected Passwords

System-selected passwords are often provided by the CSP at enrollment or by the verifier. The latter is common for PINs. The guidelines are as follows:

- The password or PIN must be at least six characters in length and may be entirely numeric.
- The password must be generated using an approved random bit generator, listed in SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*.

https://t.me/learningnets

Ideally, the generated password should be pronounceable and relatively easy to remember yet hard to guess even if the password generation algorithm is known.

10.4 Possession-Based Authentication

Objects that a user possesses for the purpose of user authentication are sometimes called *hardware tokens* (to distinguish from a number of software types of tokens). This section examines several types of hardware tokens that are widely used—cards that have the appearance and size of bank cards (see Table 10.2). It then describes another type of hardware token used for one-time password generation.

TABLE 10.2 Types of Cards Used as Possession Factors

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Traditional credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart ■ Contact ■ Contactless	Electronic memory and processor inside ■ Electrical contacts exposed on surface ■ Radio antenna embedded inside	Biometric ID card

Memory Cards

Memory cards store but do not process data. The most common such card is a bank card with a magnetic stripe on the back. A magnetic stripe stores only a simple security code, which is read (and unfortunately reprogrammed) by an inexpensive card reader. There are also memory cards that include an internal electronic memory.

Memory cards are used alone for physical access, such as a hotel room. For authentication, a user provides both the memory card and some form of password or PIN. A typical application is an automatic teller machine (ATM). The memory card, when combined with a PIN or password, provides significantly greater security than a password alone. An adversary must gain physical possession of the card (or must be able to duplicate it) and must gain knowledge of the PIN. Among the potential drawbacks are the following:

- **Special reader requirement:** This increases the cost of using the hardware token and creates the requirement to maintain the security of the reader's hardware and software.

https://t.me/learningnets

- **Hardware token loss:** A lost hardware token temporarily prevents its owner from gaining system access. Thus, there is an administrative cost in replacing the lost token. In addition, if the token is found, stolen, or forged, then an adversary needs only determine the PIN to gain unauthorized access.
- **User dissatisfaction:** Although users may have no difficulty in accepting the use of a memory card for ATM access, its use for computer access may be deemed inconvenient.

Smart Cards

A wide variety of devices qualify as smart tokens. These are categorized along four dimensions that are not mutually exclusive:

- **Physical characteristics:** A smart token includes an embedded microprocessor. A smart token that looks like a bank card is called a smart card. Other smart tokens look like calculators, keys, or other small portable objects.
- **User interface:** Manual interfaces include a keypad and display for human/token interaction.
- **Electronic interface:** A smart card or other token requires an electronic interface to communicate with a compatible reader/writer. A card may have one or both of the following types of interface:
  - **Contact:** A contact smart card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card (typically gold plated). Transmission of commands, data, and card status takes place over these physical contact points.
  - **Contactless:** A contactless card requires only close proximity to a reader. Both the reader and the card have an antenna, and the two communicate using radio frequencies. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is typically 0.5 to 3 inches for nonbattery-powered cards, which is ideal for applications such as building entry and payment that require a very fast card interface.
- **Authentication protocol:** A smart token provides a means for user authentication. The authentication protocols used with smart tokens are classified into three categories:
  - **Static:** With a static protocol, the user authenticates himself or herself to the token, and then the token authenticates the user to the computer. The latter part of this protocol is similar to the operation of a memory token.

https://t.me/learningnets

- **Dynamic password generator:** In this case, the token generates a unique password periodically (for example, every minute). This password is then entered into the computer system for authentication, either manually by the user or electronically via the token. The token and the computer system must be initialized and kept synchronized so that the computer knows the password that is current for this token.
- **Challenge-response:** In this case, the computer system generates a challenge, such as a random string of numbers. The smart token generates a response based on the challenge. For example, public-key cryptography could be used, and the token would encrypt the challenge string with the token's private key.

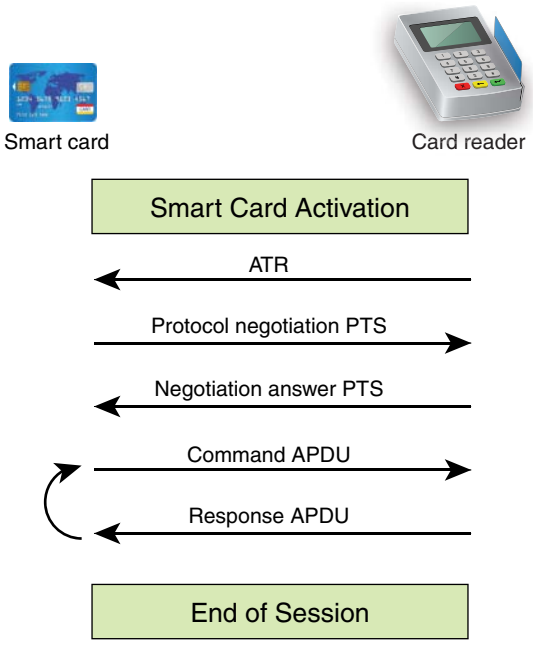
For user authentication, the most important category of smart token is the smart card, which has the appearance of a credit card, has an electronic interface, and may use any of the type of protocols just described. The remainder of this section discusses smart cards.

A smart card contains within it an entire microprocessor, including processor, memory, and I/O ports. Some versions incorporate a special coprocessing circuit for cryptographic operation to speed the task of encoding and decoding messages or generating digital signatures to validate the information transferred. In some cards, the I/O ports are directly accessible by a compatible reader by means of exposed electrical contacts. Other cards rely instead on an embedded antenna for wireless communication with the reader.

A typical smart card includes three types of memory. Read-only memory (ROM) stores data that does not change during the card's life, such as the card number and the cardholder's name. Electrically erasable programmable ROM (EEPROM) holds application data and programs, such as the protocols that the card can execute. It also holds data that may vary with time. For example, in a telephone card, the EEPROM holds the talk time remaining. Random access memory (RAM) holds temporary data generated when applications are executed.

Figure 10.5 illustrates the typical interaction between a smart card and a reader or computer system. Each time the card is inserted into a reader, a reset is initiated by the reader to initialize parameters such as clock value. After the reset function is performed, the card responds with an answer to reset (ATR) message. This message defines the parameters and protocols that the card can use and the functions it can perform. The terminal is able to change the protocol used and other parameters via a protocol type selection (PTS) command. The cards PTS response confirms the protocols and parameters to be used. The terminal and card now execute the protocol to perform the desired application.

https://t.me/learningnets



APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection

FIGURE 10.5 Smart Card/Reader Exchange

Electronic Identity Cards

An application of increasing importance is the use of smart cards as national ID cards for citizens. A national electronic identity (eID) card serve the same purposes as other national ID cards and similar cards, such as driver's licenses, for access to government and commercial services. In addition, an eID card provides stronger proof of identity and is used in a wider variety of applications. In effect, an eID card is a smart card that was verified by the national government as being valid and authentic.

One of the most recent and most advanced eID deployments is the German eID card *neuer Personalausweis* [POLL12]. The card has human-readable data printed on its surface, including the following:

- **Personal data:** Name, date of birth, and address—the type of printed information found on passports and driver's licenses
- **Document number:** An alphanumerical nine-character unique identifier

https://t.me/learningnets

- **Card access number (CAN):** A six-digit decimal random number printed on the face of the card that is used as a password
- **Machine-readable zone (MRZ):** Three lines of human- and machine-readable text on the back of the card that can also be used as a password

eID Functions

An eID card has three separate electronic functions, each with its own protected data set, as shown in Table 10.3.

TABLE 10.3 Electronic Functions and Data for eID Cards

Function	Purpose	PACE Password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data.	Card access number or machine-readable zone	Face image, two fingerprint images (optional), machine-readable zone data	Offline biometric identity verification reserved for government access
eID (activation optional)	Online applications read the data or access functions as authorized.	eID PIN	Family and given names, artistic name and doctoral degree, date and place of birth, address and community ID, expiration date	Identification, age verification, community ID verification, restricted identification (pseudonym), revocation query
	Offline inspection systems read the data and update the address and community ID.	Card access number or machine-readable zone		
eSign (certificate optional)	A certification authority installs the signature certificate online.	eID PIN	Signature key, X.509 certificate	Electronic signature creation
	Citizens make electronic signatures with eSign PINs.	Card access number		

The three separate electronic functions are as follows:

- **ePass:** This function is reserved for government use and stores a digital representation of the cardholder's identity. This function is similar to, and may be used for, an electronic passport. Other government services also use ePass. The ePass function must be implemented on the card.

https://t.me/learningnets

- **eID:** This function is for general-purpose use in a variety of government and commercial applications. The eID function stores an identity record that authorized service accesses with cardholder permission. Citizens choose whether they want this function activated.
- **eSign:** This optional function stores a private key and a certificate verifying the key; it is used for generating a digital signature. A private-sector trust center issues the certificate.

The ePass function is an offline function. That is, it is not used over a network but is used in a situation where the cardholder presents the card for a particular service at that location, such as going through a passport control checkpoint.

The eID function is used for both online and offline services. An example of an offline use is an inspection system. An inspection system is a terminal for law enforcement checks, for example, by police or border control officers. An inspection system reads identifying information of the cardholder as well as biometric information stored on the card, such as facial image and fingerprints. The biometric information is used to verify that the individual in possession of the card is the actual cardholder.

User authentication is a good example of online use of the eID function. Figure 10.6 illustrates a web-based scenario. To begin, an eID user visits a website and requests a service that requires authentication. The website sends back a redirect message that forwards an authentication request to an eID server. The eID server requests that the user enter the PIN for the eID card. Once the user has correctly entered the PIN, data is exchanged between the eID card and the terminal reader in encrypted form. The server then engages in an authentication protocol exchange with the microprocessor on the eID card. If the user is authenticated, the results are sent back to the user system to be redirected to the web server application.

For the preceding scenario, the appropriate software and hardware are required on the user system. Software on the main user system includes functionality for requesting and accepting the PIN and for message redirection. The hardware required is an eID card reader. The card reader is either an external contact or contactless reader or a contactless reader internal to the user system.

Password Authenticated Connection Establishment (PACE)

PACE ensures that the contactless radio-frequency (RF) chip in the eID card cannot be read without explicit access control. For online applications, access to the card is established by the user entering the six-digit PIN, which should only be known to the holder of the card. For offline applications, either the MRZ printed on the back of the card or the six-digit CAN printed on the front is used.

https://t.me/learningnets

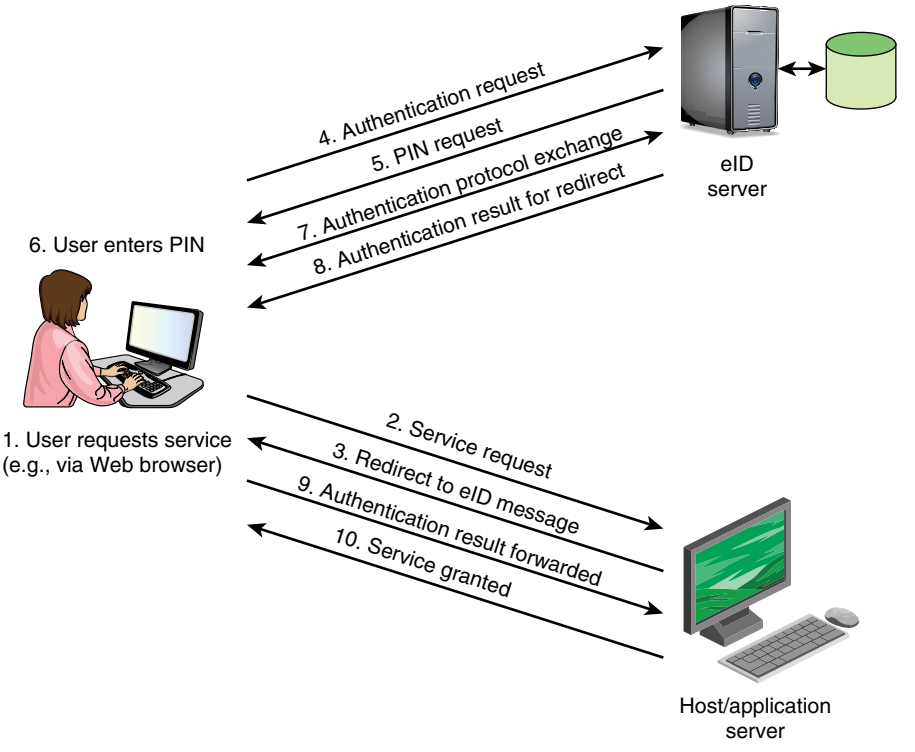


FIGURE 10.6 User Authentication with eID

One-Time Password Device

An increasingly widespread device used for authentication is a key fob type of device that generates one-time passwords. The use of a one-time password (OTP) improves security, preventing the risk of guessing and reusing a password, especially if used together with other authentication mechanisms. The OTP device supports the spontaneous generation of one-time passwords. This device has an embedded secret that is used as the seed for generation of one-time passwords and may not require activation through a second factor. Authentication is accomplished by providing an acceptable one-time password and thereby proving possession and control of the device.

In the most widely used version of the OTP device, a user is supplied with a physical card or other hardware token that displays a new pseudo-random number at frequent intervals (usually one minute). To authenticate, the user types both the currently displayed pseudo-random number and a PIN that the user must remember. Thus, this is two-factor authentication.

A popular two-factor OTP device is the RSA SecurID product. The device uses a built-in clock and the device's factory-encoded random key (known as the seed). The seed, which

https://t.me/learningnets

is different for each device, is loaded into the corresponding RSA SecurID server (RSA Authentication Manager, formerly ACE/Server) as the hardware tokens are purchased. The seed initiates a random number generator that produces numbers such that knowledge of one number is insufficient to guess the next number in the sequence. The server, which also has a real-time clock and a database of valid cards with the associated seed records, authenticates a user by computing what number the token is supposed to be showing at that moment in time and checking this against what the user entered.

The RSA SecurID scheme also supports two additional challenge-response modes:

- **Next token mode:** Applied in cases where the authentication process requires additional verification of the token code. The user is challenged to enter the next token code—that is, to wait for the number that is displayed on the authenticator to change and enter the new number (without the PIN). Next token mode occurs for three common reasons:
  - The first use of a token requires a resynchronization.
  - The user has entered too many incorrect passcodes.
  - The token presented to the AM server is outside the automatic acceptance range (typically the previous token code, the expected token code, and the next token code).
- **New PIN mode:** Applied in cases where the authentication process requires additional verification of the PIN. In this case, the user must use a new PIN. Depending on the configuration of the RSA ACE/Server, the user is prompted to select and enter a new PIN or the server supplies the user with a new PIN. The user then reauthenticates with the new PIN. New PIN mode occurs because the user's token is not yet associated with a PIN, which is required for two-factor authentication. All new tokens are in this mode, even replacement tokens.

Threats to Possession-Based Authentication

Hardware tokens are vulnerable to a variety of threats, including the following:

- **Theft:** An attacker can steal a token device. If a second factor is required, such as a PIN, the attacker must also use some means to obtain or guess the PIN. If the second factor is biometric, the attacker must come up with some way of forging the biometric characteristic.
- **Duplication:** The attacker gains access to the device and clones it. Again, if a second factor is required, the attacker's task is more formidable.
- **Eavesdropping/replaying:** The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating. This captured information can be used later. If there is a time-sensitive aspect to the exchange, such a nonce or the use of an OTP, this latter attack can be thwarted.

https://t.me/learningnets

- **Replay:** If the attacker can interpose between the token device and the server, then this constitutes a man-in-the-middle (MITM) attack, in which the attacker assumes the role of the client to the server and the server to the client.
- **Denial of service:** Repeated failed attempts by the attacker to the server may cause the server to lock out the legitimate client.
- **Host attack:** The attacker may gain sufficient control of the authentication server for the attacker to be authenticated to an application.

Security Controls for Possession-Based Authentication

A number of security controls enhance the security of hardware tokens, including the following:

- Use multifactor hardware tokens that need to be activated through a PIN or biometric.
- Use hardware tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. The random number generator in SecurID is an example.
- Use a hardware token that locks up after a number of repeated failed activation attempts.
- Include theft prevention in user training and awareness programs.
- Require individuals to take specific security safeguards to protect token devices.
- Verify, as part of the initial token device distribution, the identity of the individual receiving the authenticator.
- Ensure that authenticators have sufficient strength of mechanism for their intended use.
- Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
- Establish maximum lifetime restrictions and reuse conditions for token devices.

10.5 Biometric Authentication

A biometric authentication system attempts to authenticate an individual based on his or her unique physical characteristics. These include both static characteristics (for example, fingerprints, hand geometry, facial characteristics, retinal and iris

https://t.me/learningnets

patterns) and dynamic characteristics (for example, voiceprint, signature). In essence, biometrics is based on pattern recognition. Compared to passwords and hardware tokens, biometric authentication is both technically complex and expensive. While it is used in a number of specific applications, biometrics has yet to mature as a standard tool for user authentication to computer systems. Accordingly, SP 800-63 does not support the use of biometric authentication alone.

Criteria for Biometric Characteristics

In designing a biometric identification system, two sets of criteria must be considered: the nature of the biometric feature and requirements for a biometric system. With respect to biometric features, such features must have the following properties:

- **Universality:** A very high percentage of the population, approaching 100%, should have the characteristic. For example, virtually everyone has recognizable fingerprints, though there are rare exceptions.
- **Distinctiveness:** No two people should have identical characteristics. For some otherwise acceptable characteristics, identical twins share virtually the same patterns, such as facial features and DNA, but not other features, such as fingerprints and iris patterns.
- **Permanence:** The characteristic should not change with time. For otherwise acceptable characteristics, such as facial features and signatures, periodic re-enrollment of the individual may be required.
- **Collectability:** Obtaining and measuring the biometric feature(s) should be easy, non-intrusive, reliable, and robust, as well as cost-effective for the application.

A biometric identification system should also meet the following system criteria:

- **Performance:** The system must meet a required level of accuracy, perform properly in the required range of environments, and be cost-effective.
- **Circumvention:** The difficulty of circumventing the system must meet a required threshold. This is particularly important in an unattended environment, where it is easier to use such countermeasures and a fingerprint prosthetic or a photograph of a face.
- **Acceptability:** The system must be generally acceptable to users. Systems that are uncomfortable for the user, appear threatening, require contact that raises hygienic issues, or are basically non-intuitive are likely not to be acceptable to the general population.

https://t.me/learningnets

Physical Characteristics Used in Biometric Applications

A number of different types of physical characteristics are either in use or under study for user authentication. The most common are the following:

- **Facial characteristics:** Facial characteristics are the most common means of human-to-human identification; thus, it is natural to consider them for identification by computer. The most common approach is to define characteristics based on relative location and shape of key facial features, such as eyes, eyebrows, nose, lips, and chin shape. An alternative approach is to use an infrared camera to produce a face thermogram that correlates with the underlying vascular system in the human face.
- **Fingerprints:** Fingerprints have been used as a means of identification for centuries, and the process has been systematized and automated particularly for law enforcement purposes. A fingerprint is the pattern of ridges and furrows on the surface of the fingertip. Fingerprints are believed to be unique across the entire human population. In practice, automated fingerprint recognition and matching system extract a number of features from the fingerprint for storage as a numerical surrogate for the full fingerprint pattern. In recent years, advances in recognition technology have resulted in accuracy rates exceeding 99% for automated fingerprint systems [NSTC11].
- **Hand geometry:** Hand geometry systems identify features of the hand, including shape and lengths and widths of fingers.
- **Retinal pattern:** The pattern formed by veins beneath the retinal surface is unique and therefore suitable for identification. A retinal biometric system obtains a digital image of the retinal pattern by projecting a low-intensity beam of visual or infrared light into the eye.
- **Iris:** Another unique physical characteristic is the detailed structure of the iris. There has been a lot of research in this area, with significant gains in recent years in both capture devices and recognition algorithms [NSTC11]. Newer cameras have much lower failure-to-capture rates and transaction times, and some have the ability to collect iris images at a distance and in motion. Recent research [GRAH12] indicates that iris patterns change as the eye ages, so the need to retake iris patterns after a long period may be necessary.
- **Signature:** Each individual has a unique style of handwriting and this is reflected especially in the signature, which is typically a frequently written sequence. However, multiple signature samples from a single individual are not identical. This complicates the task of developing a computer representation of the signature to be matched to future samples.

https://t.me/learningnets

- **Voice:** Whereas the signature style of an individual reflects not only the unique physical attributes of the writer but also the writing habit that has developed, voice patterns are more closely tied to the physical and anatomical characteristics of the speaker. Nevertheless, there is still a variation from sample to sample over time from the same speaker, complicating the biometric recognition task.

Figure 10.7 gives a rough indication of the relative cost and accuracy of these biometric measures. The concept of accuracy does not apply to user authentication schemes using smart cards or passwords. For example, if a user enters a password, it either matches exactly the password expected for that user or not. In the case of biometric parameters, the system instead must determine how closely a presented biometric characteristic matches a stored characteristic. Before elaborating on the concept of biometric accuracy, you need to have a general idea of how biometric systems work.

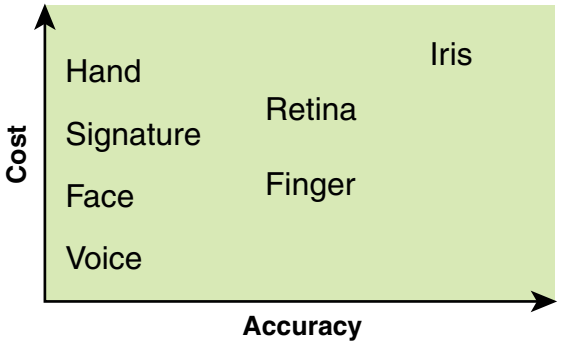


FIGURE 10.7 Cost Versus Accuracy of Various Biometric characteristics in User Authentication Schemes

Operation of a Biometric Authentication System

Figure 10.8 illustrates the operation of a biometric system. Each individual to be included in the database of authorized users must first be *enrolled* in the system. This is analogous to assigning a password to a user. For a biometric system, the user presents a name and, typically, some type of password or PIN to the system. At the same time, the system senses some biometric characteristic of this user (for example, fingerprint of the right index finger). The system digitizes the input and then extracts a set of features that are stored either as a number or set of numbers representing

https://t.me/learningnets

this unique biometric characteristic; this set of numbers is referred to as the user's template. The user is now enrolled in the system, which maintains for the user a name (ID), perhaps a PIN or password, and the biometric value.

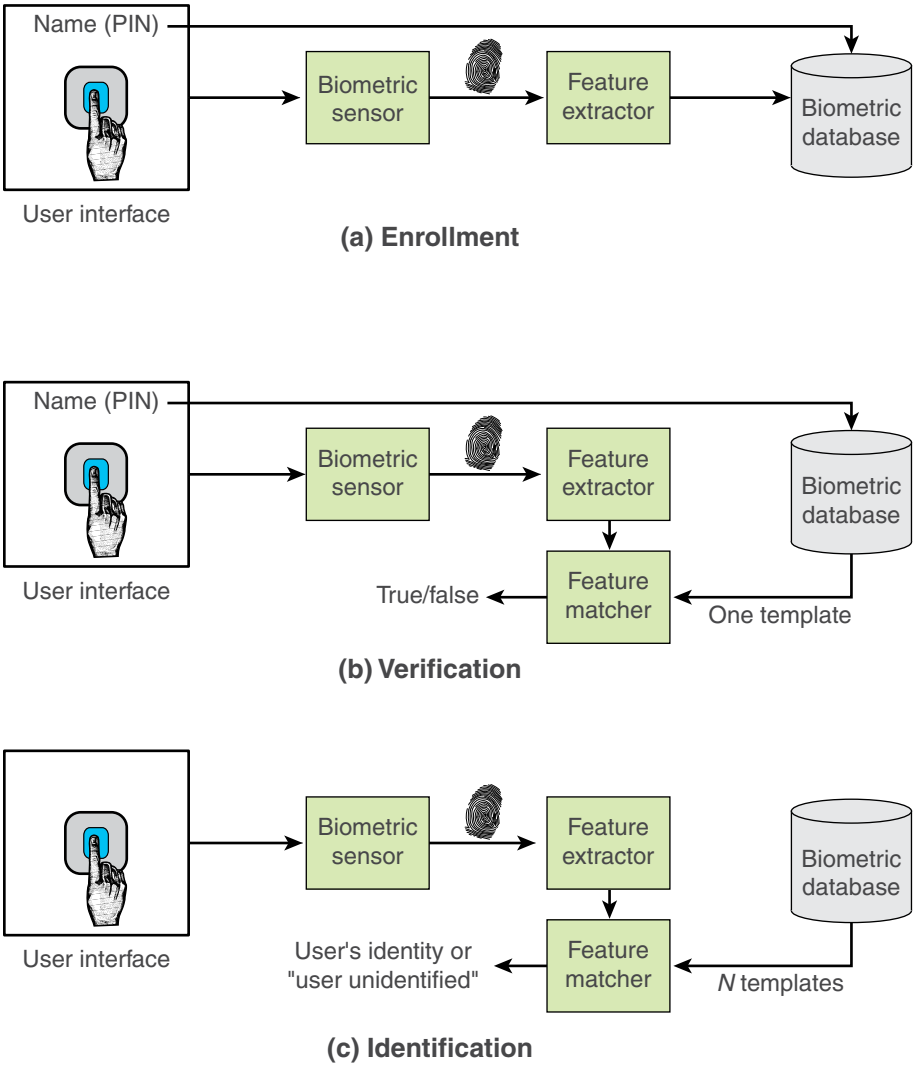


FIGURE 10.8 Generic Biometric Scheme

Depending on the application, user authentication on a biometric system involves either *verification* or *identification*. Verification is analogous to a user logging on to a system by using a memory card or smart card coupled with a password or PIN.

https://t.me/learningnets

For biometric verification, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding feature and compares that to the template stored for this user. If there is a match, then the system authenticates this user.

For an identification system, the individual uses the biometric sensor but presents no additional information. The system then compares the presented template with the set of stored templates. If there is a match, then this user is identified. Otherwise, the user is rejected.

Biometric Accuracy

In any biometric scheme, some physical characteristic of the individual is mapped into a digital representation. For each individual, a single digital representation, or template, is stored in the computer. When the user is to be authenticated, the system compares the stored template to the presented template. Given the complexities of physical characteristics, do not expect it to be an exact match between the two templates. Rather, the system uses an algorithm to generate a matching score (typically a single number) that quantifies the similarity between the input and the stored template. To proceed with the discussion, we need to define a couple terms. The *false match rate* (*FMR*) is the frequency with which biometric samples from different sources are erroneously assessed to be from the same source. The *false nonmatch rate* (*FNMR*) is the frequency with which samples from the same source are erroneously assessed to be from different sources.

Figure 10.9 illustrates the dilemma posed to the system. If a single user is tested by the system numerous times, the matching score s will vary, with a probability density function typically forming a bell curve, as shown. For example, in the case of a fingerprint, results can vary due to sensor noise, changes in the print due to swelling or dryness, finger placement, and so on. On average, any other individual would have a much lower matching score but again exhibit a bell-shaped probability density function. The difficulty is that the range of matching scores produced by two individuals, one genuine and one an imposter, compared to a given reference template, are likely to overlap. In Figure 10.9 a threshold value is selected such that if the presented value $s \geq t$, a match is assumed, and for $s < t$, a mismatch is assumed. The shaded part to the right of t indicates a range of values for which a false match is possible, and the shaded part to the left indicates a range of values for which a false nonmatch is possible. A false match results in the acceptance of a user who should not be accepted, and a false mismatch triggers the rejection of a valid user. The area of each shaded part represents the probability of a false match or nonmatch, respectively. By moving the threshold left or right,

https://t.me/learningnets

the probabilities can be altered, but note that a decrease in the FMR results in an increase in the FNMR and vice versa.

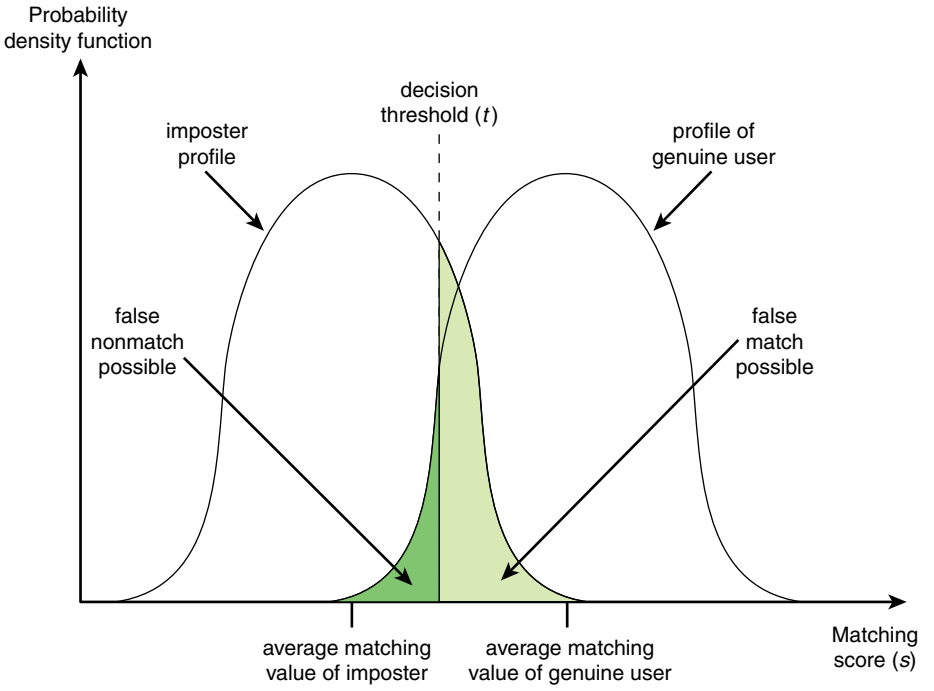


FIGURE 10.9 Profiles of a Biometric Characteristic of an Imposter and an Unauthorized User

For a given biometric scheme, plot the FMR versus the FNMR to obtain the *operating characteristic curve*. Figure 10.10 shows idealized curves for two different systems. The curve that is lower and to the left performs better. The dot on the curve corresponds to a specific threshold for biometric testing. Shifting the threshold along the curve up and to the left provides greater security and the cost of decreased convenience. The inconvenience comes from a valid user being denied access and being required to take further steps. A plausible trade-off is to pick a threshold that corresponds to a point on the curve where the rates are equal. A high-security application can require a very low FMR, resulting in a point farther to the left on the curve. For a forensic application, in which the system is looking for possible candidates, to be checked further, the requirement can be for a low FNMR.

https://t.me/learningnets

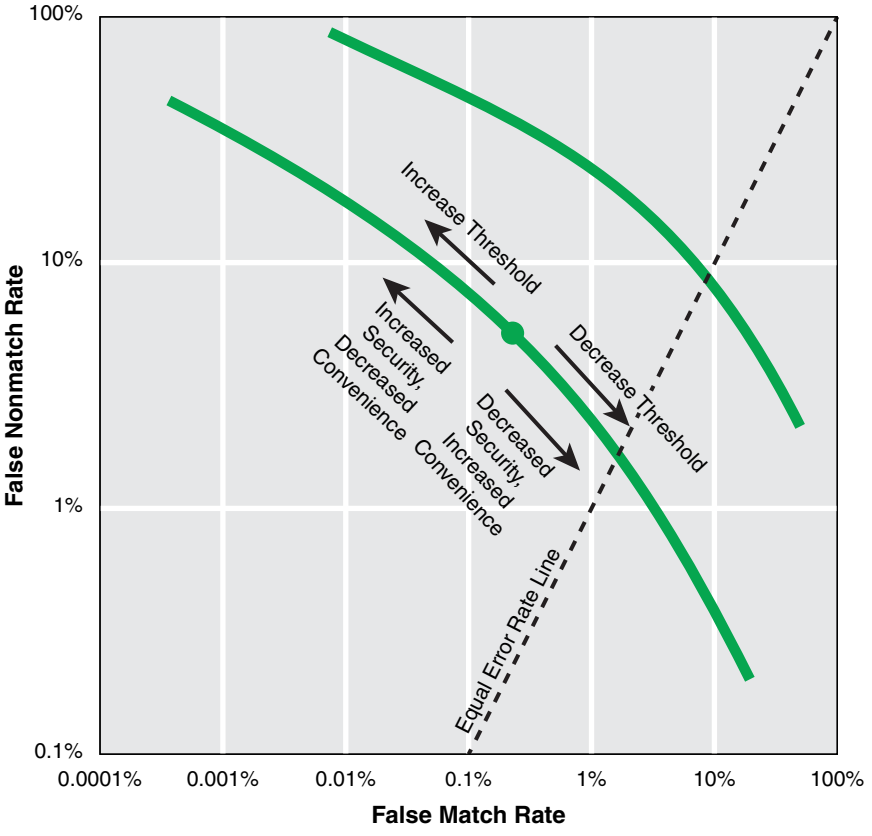


FIGURE 10.10 Idealized Biometric Measurement Operating Characteristic Curves (Log-Log Scale)

Threats to Biometric Authentication

During biometric authentication of the type illustrated in Figure 10.8b, a typical sequence of steps is as follows:

1. A biometric pattern is presented.
2. That data is captured via a sensor.
3. Signal processing of captured data to extract features typically takes place.
4. A comparison of the captured data occurs, against templates of user biometric characteristics retrieved from storage.
5. An authentication decision is made.

https://t.me/learningnets

attack surface
The reachable and exploitable vulnerabilities in a system.

Figure 10.11, based on figures in Ratha et al.'s "Enhancing Security and Privacy in Biometrics-Based Authentication Systems" [RATH01] and NIST's *Measuring Strength of Authentication* [NIST15], depicts 11 **attack surface** points in a system where an attacker could potentially interject into the flow to interfere with the authentication decision. These 11 elements may all be self-contained within a single device (such as a mobile device) or distributed across multiple physical systems.

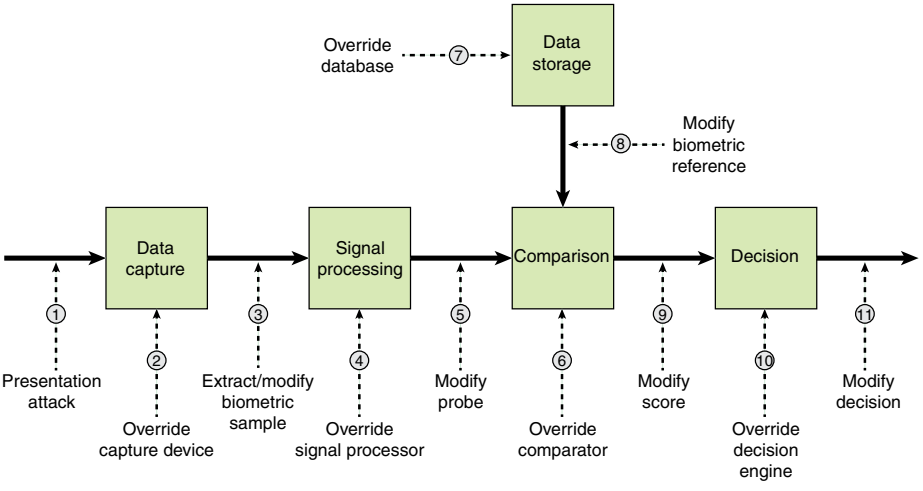


FIGURE 10.11 Biometric System Attack Diagram

The following list summarizes the nature of the potential attack at each point (numbers corresponded to circled numbers in figure):

1. An attacker may present a fake biometric to a sensor.
2. An attacker may modify hardware/software in the data capture device.
3. A replay attack is possible here, in which the attacker resubmits a previously stored digitized biometric signal.
4. An attacker may modify hardware/software in the signal-processing device. For example, the feature extractor may be attacked using a Trojan horse so that it produces feature sets preselected by the intruder.
5. If the signal processor and comparator are physically separate, an attacker could interpose on the communications path and replace the extracted features with a different, fraudulent feature set.
6. A comparison algorithm compares an input from the sensor to a stored biometric sample for a user. The performance of the comparator depends on two major factors: how distinctive the biometric pattern is (that is, the modality's

https://t.me/learningnets

innate features and how many distinct individual patterns may exist) and the approach of a vendor's algorithm to analyze the modality. An attacker could attempt to modify or otherwise disrupt the algorithm.

7. An attacker may attempt to extract and modify stored information.
8. An attacker may attack the channel between the stored templates and the matcher. In this case, the stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified.
9. The result of the comparison algorithm is a match score between two biometric samples: the one presented by the user and the one in the template database. If the comparison algorithm and the decision engine are physically separate, as match scores are sent to the decision engine, that channel must prevent the modification of any data.
10. An attacker may modify hardware/software in the decision engine.
11. An attacker may intercept a decision communicated by the decision engine and alter it.

Many of these vulnerabilities fall into familiar categories that are common in other authentication systems, such as protecting data in transit or at rest, and the cybersecurity controls discussed throughout this book can mitigate such risks for biometric systems in the same way as other information systems. There are two notable vulnerabilities that fall outside the protection provided by core cybersecurity controls:

- **Presentation attack:** The principal source of vulnerability not covered by core cybersecurity controls is known as a presentation attack. This type of attack attempts to mimic a biometric feature to sufficient fidelity so it is accepted as valid by the system—an attack known as *biometric spoofing*. There is added risk in uncontrolled environments where there is not an operator to monitor the presentation of a biometric.
- **Override comparator:** In addition to introducing malware to modify the behavior of the comparator, an attacker can attempt to take advantage of characteristics of the specific comparison algorithm. Flaws discovered in the algorithm can make the biometric spoofing easier.

Security Controls for Biometric Authentication

The most important security control for biometric authentication is presentation attack detection (PAD). This section looks at PAD and then provides general guidelines for securing biometric authentication.

https://t.me/learningnets

Presentation Attack Detection

PAD involves two types of methods to directly counter spoof attempts at the biometric sensor: artifact detection and liveness detection. *Artifact detection* attempts to answer the question "Is the biometric sample at the sensor artificial?" For example, for a voice detector, is it a human voice or a voice produced by a voice synthesizer? *Liveness detection* attempts to answer the question: "Is the biometric sample at the sensor from a living human presenting a sample to be captured?" For example, is it a fingerprint sensed from the user's finger, or is it a fingerprint presented by the lift of a fingerprint onto a printed surface?

PAD error rates must be determined through empirical testing. The goal for PAD testing is to test a set of materials that represent an attack potential level and determine the maximum error rate found among those materials. Attack potential levels represent increasing levels of effort to mount an attack. For a given biometric system, the security officer needs to determine for what attack potential level it is worthwhile to develop security controls. See NIST's *Strength of Function for Authenticators—Biometrics (SOFA-B): Discussion Draft Open for Comments* [NIST17] for a discussion of attack potential levels and the security approached that is recommended.

NIST Guidelines

NIST SP 800-63B supports only limited use of biometrics for authentication for the following reasons:

- Biometric comparison is probabilistic, whereas other authentication factors are deterministic. Thus, the FMR does not provide confidence in the subscriber when the biometric is used alone.
- The FMR does not account for biometric spoofing.
- Biometric template protection schemes provide a method for revoking biometric credentials that is comparable to other authentication factors (for example, PKI certificates and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.
- Biometric characteristics do not constitute secrets. They are either obtained online or by taking a picture of someone with a camera phone (for example, facial images) with or without their knowledge, lifted from objects someone touches (for example, latent fingerprints), or captured with high-resolution images (for example, iris patterns). While PAD technologies mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the security needs of the organization.

https://t.me/learningnets

Accordingly, SP 800-63B includes the following guidelines for use of biometric authentication:

- Biometrics must only be used as part of a multifactor scheme that includes a hardware token authenticator.
- The FMR for the biometric system must be less than or equal to 1/1000 under a zero-effort imposter attempt. A zero-effort imposter attempt occurs when an individual submits his or her own biometric characteristics as if he or she were attempting successful verification against his or her own template, but the comparison is made against the template of another user.
- The biometric system should implement PAD and have a demonstrated success rate of at least 90%.

10.6 Risk Assessment for User Authentication

As described in Chapter 3, "Information Risk Assessment," risk assessment is the overall process of risk identification, risk analysis, and risk evaluation. This section examines aspects of risk assessment related to user authentication.

Authenticator Assurance Levels

NIST SP 800-63 provides a useful way of characterizing the risk of an authentication system, using the concept of *authentication assurance level* (*AAL*). A higher AAL indicates that an attacker must have better capabilities and expend greater resources to successfully subvert the authentication process. NIST SP 800-63B specifies the types of security controls, in terms of authentication factors, that correspond to the three defined AALs. Thus, the management can assess the level of risk for various levels of resources devoted to security controls and decide what controls are needed to satisfy the organization's risk requirement for authentication in various contexts.

The three AALs, from lowest to highest, are:

- **AAL1:** Provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multifactor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- **AAL2:** Provides high confidence that the claimant controls the authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors are required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and AAL3.

https://t.me/learningnets

- **AAL3:** AAL3 provides very high confidence that the claimant controls the authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication requires use of a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both of these requirements. In order to authenticate at AAL3, claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

Selecting an AAL

To determine the appropriate AAL for user authentication, the responsible person should estimate the impact on the organization using the three risk levels defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (low, moderate, and high). SP 800-63 defines six categories of harm and defines the impact levels as follows:

- Potential impact of inconvenience, distress, or damage to standing or reputation:
  - **Low:** At worst, limited, short-term inconvenience, distress, or embarrassment to any party.
  - **Moderate:** At worst, serious short-term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
  - **High:** Severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is ordinarily reserved for situations with particularly severe effects or that potentially affect many individuals.
- Potential impact of financial loss:
  - **Low:** At worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
  - **Moderate:** At worst, a serious financial loss to any party or a serious agency liability.
  - **High:** Severe or catastrophic financial loss to any party or severe or catastrophic agency liability.
- Potential impact of harm to agency programs or public interests:
  - **Low:** At worst, a limited adverse effect on organizational operations or assets or public interests. Examples of limited adverse effects are mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness or minor damage to organizational assets or public interests.

https://t.me/learningnets

- **Moderate:** At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness or significant damage to organizational assets or public interests.
- **High:** A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions or major damage to organizational assets or public interests.

- Potential impact of unauthorized release of sensitive information:
  - **Low:** At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact, as defined in FIPS 199.
  - **Moderate:** At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact, as defined in FIPS 199.
  - **High:** A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact, as defined in FIPS 199.
- Potential impact to personal safety:
  - **Low:** At worst, minor injury not requiring medical treatment.
  - **Moderate:** At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
  - **High:** A risk of serious injury or death.
- Potential impact of civil or criminal violations:
  - **Low:** At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
  - **Moderate:** At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
  - **High:** A risk of civil or criminal violations that are of special importance to enforcement programs.

Table 10.4, adapted from SP 800-63, shows the mapping between each category of harm and the corresponding recommended minimum AAL to employ. Note that there is not a simple one-to-one correspondence. For example, if there is a low risk to personal safety, the recommendation is to use AAL2 rather than AAL1.

https://t.me/learningnets

TABLE 10.4 Assurance Level Determined by Estimated Impact Level

	Impact Levels (FIPS 199)		
Impact Category	**Low**	**Moderate**	**High**
Inconvenience, distress, or damage to standing or reputation	AAL1	AAL2	AAL3
Financial loss or agency liability	AAL1	AAL2	AAL3
Harm to agency programs or public interests	AAL2	AAL2	AAL3
Unauthorized release of sensitive information	AAL2	AAL2	AAL3
Personal safety	AAL2	AAL3	AAL3
Civil or criminal violations	AAL2	AAL2	AAL3

In essence, the level assigned should be the highest level found for any of the six categories of harm. If the level is AAL1, then a further consideration is made concerning privacy. If personal data are made accessible, then at least AAL 2 should be used. Figure 10.12, from SP 800-63, shows the decision process just described.

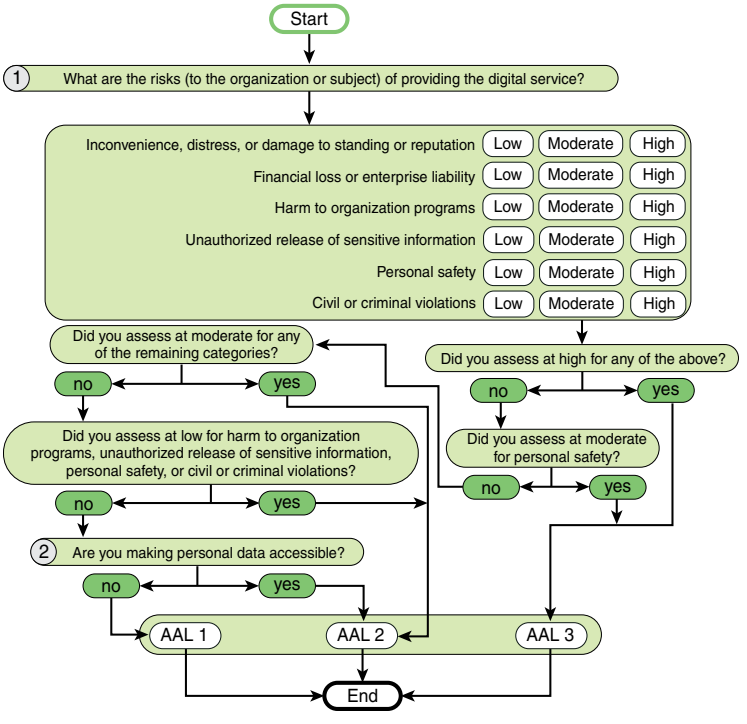


FIGURE 10.12 *Selecting the AAL*

https://t.me/learningnets

Choosing an Authentication Method

SP 800-63B defines nine different authentication types that can be used alone or in combination to construct an authentication method:

- **Memorized secret:** A password or PIN.
- **Lookup secret:** A physical or electronic record that stores a set of secrets shared between the claimant and the CSP. The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. This is similar in concept to a **one-time pad**.
- **Out-of-band device:** A physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel referred to as the *secondary channel*. The device is possessed and controlled by the claimant and supports private communication over this secondary channel, separate from the primary channel for e-authentication.
- **Single-factor OTP device:** A one-time password used as the only factor for authentication. Described in Section 10.4.
- **Multifactor OTP device:** A device similar manner to a single-factor OTP device, except that it requires the entry of either a memorized secret or the use of a biometric to obtain the one-time password.
- **Single-factor cryptographic software:** A cryptographic key stored on disk or some other soft media. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message using public key cryptography.
- **Single-factor cryptographic device:** A hardware device that performs cryptographic operations using protected cryptographic key(s) and provides the authenticator output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second factor of authentication. Authentication is accomplished by proving possession of the device via the authentication protocol.
- **Multifactor cryptographic software:** Software similar to single-factor cryptographic software but that requires a second authentication factor to activate.
- **Multifactor cryptographic device:** A device similar to a single-factor cryptographic device but that requires a second authentication factor to activate.

one-time pad
An encryption scheme in which the key length is equal to the message length, with each element (bit or character) of the key used to encrypt/decrypt each element of the message (e.g., by XOR). The key is randomly chosen and used only once, for a single message. If the key is secure, this scheme is impossible to break.

Once the authentication level is determined, the choice of authentication method consists of one or a combination of the above authenticator types. For AAL1, any of the nine types can be used by itself, reflecting the fact that less security is required than at higher

https://t.me/learningnets

levels. For AAL2, there are two main options. The first is to use hardware or software that combines two factors of authentication. The second is to combine a password with an authenticator type that is single factor. For AAL3, to achieve high confidence, it must include proof of possession of a key through a cryptographic protocol plus an authenticator that secures against an impersonation of the verifier entity.

Table 10.5 summarizes the options for the three assurance levels. The upper part of the table shows the options for AAL1 and the two sets of options for AAL2. The lower part of the table shows the six sets of options for AAL3. A single checkmark in a column indicates that that type is required; multiple checkmarks in a column indicate that exactly one of the types is required. For AAL2, the memorized secret type is required (R) plus exactly one of the types indicated by a checkmark. For options 2 through 6 of AAL3, all of the indicated authenticators (A) in a column are required.

TABLE 10.5 AAL by Authenticator Type

(a) Options for AAL1 and AAL2

Authenticator Type	AAL1	AAL2 (using a multi-factor authenticator)	AAL2 (using two single-factor authenticators)
Memorized secret	✓		**R**
Lookup secret	✓		✓
Out-of-band device	✓		✓
Single-factor OTP device	✓		✓
Multifactor OTP device	✓	✓	
Single-factor cryptographic software	✓		✓
Single-factor cryptographic device	✓		✓
Multifactor cryptographic software	✓	✓	
Multifactor cryptographic device	✓	✓	

(b) Options for AAL3

Authenticator Type	AAL3 Option 1	AAL3 Option 2	AAL3 Option 3	AAL3 Option 4	AAL3 Option 5	AAL3 Option 6
Memorized secret		**A**				**A**
Lookup secret						
Out-of-band device						

https://t.me/learningnets

Authenticator Type	AAL3 Option 1	AAL3 Option 2	AAL3 Option 3	AAL3 Option 4	AAL3 Option 5	AAL3 Option 6
Single-factor OTP device					**A**	**A**
Multifactor OTP device			**A**	**A**		
Single-factor cryptographic software				**A**		**A**
Single-factor cryptographic device		**A**	**A**			
Multifactor cryptographic software					**A**	
Multifactor cryptographic device	✓					

✓ = choose one of these authenticators

R = required (plus one of the indicated authenticators)

A = all of the indicated authenticators in this column required

10.7 Access Control

This section provides an overview of important aspects of access control. It is useful to begin by defining the following terms:

- **Access:** Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
- **Access control:** The process of granting or denying specific requests for obtaining and using information and related information processing services to enter specific physical facilities.
- **Access control mechanism:** Security safeguards (that is, hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.
- **Access control service:** A security service that protects against a system entity using a system resource in a way not authorized by the system's security policy.

https://t.me/learningnets

Subjects, Objects, and Access Rights

The basic elements of access control are subject, object, and access right.

A *subject* is an entity capable of accessing objects. Generally, the concept of subject equates with that of process. Any user or application actually gains access to an object by means of a process that represents that user or application. The process takes on the attributes of the user, such as access rights.

A subject is typically held accountable for the actions he or she has initiated, and an audit trail can be used to record the association of a subject with security-relevant actions performed on an object by the subject.

Basic access control systems typically define three classes of subject, with different access rights for each class:

- **Owner:** This can be the creator of a resource, such as a file. For system resources, ownership can belong to a system administrator. For project resources, a project administrator or leader can be assigned ownership.
- **Group:** In addition to the privileges assigned to an owner, a named group of users can also be granted access rights, such that membership in the group is sufficient to exercise these access rights. In most schemes, a user may belong to multiple groups.
- **World:** The least amount of access is granted to users who are able to access the system but are not included in the categories owner and group for this resource.

An *object* is a resource to which access is controlled. In general, an object is an entity used to contain and/or receive information. Examples include records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs. Some access control systems also encompass bits, bytes, words, processors, communication ports, clocks, and network nodes.

The number and types of objects to be protected by an access control system depends on the environment in which access control operates and the desired trade-off between security on the one hand and complexity, processing burden, and ease of use on the other hand.

An *access right* describes the way in which a subject may access an object. Access rights include the following:

- **Read:** User views information in a system resource (for example, a file, selected records in a file, selected fields within a record, or some combination). Read access includes the ability to copy or print.

https://t.me/learningnets

- **Write:** User adds, modifies, or deletes data in system resource (for example, files, records, programs). Write access includes read access.
- **Execute:** User executes specified programs.
- **Delete:** User deletes certain system resources, such as files or records.
- **Create:** User creates new files, records, or fields.
- **Search:** User lists the files in a directory or otherwise search the directory.

Access Control Policies

An access control policy dictates what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following categories:

- **Discretionary access control (DAC):** Access control based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
- **Mandatory access control (MAC):** Access control based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed *mandatory* because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.
- **Role-based access control (RBAC):** Access control based on user roles (that is, a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions can be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role can apply to a single individual or to several individuals.
- **Attribute-based access control (ABAC):** Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access takes place.

DAC is the traditional method of implementing access control. MAC is a concept that evolved out of requirements for military information security. Both RBAC and ABAC have become increasingly popular.

These four policies are not mutually exclusive. An access control mechanism can employ two or even all three of these policies to cover different classes of system resources.

https://t.me/learningnets

Discretionary Access Control

A general approach to DAC, as exercised by an operating system or a database management system, is to use an *access matrix*. One dimension of the matrix consists of identified subjects that may attempt data access to the resources. Typically, this list consists of individual users or user groups, although access can be controlled for terminals, network equipment, hosts, or applications instead of or in addition to users. The other dimension lists the objects that can be accessed. At the greatest level of detail, objects can be individual data fields. More aggregate groupings, such as records, files, or even the entire database, can also be objects in the matrix. Each entry in the matrix indicates the access rights of a particular subject for a particular object.

Figure 10.13a is a simple example of an access matrix. As shown here, user A owns files 1 and 3 and has read and write access rights to those files. User B has read access rights to file 1, and so on.

In practice, an access matrix is usually sparse and is implemented by decomposition in one of two ways. The matrix can be decomposed by columns, yielding *access control lists* (*ACLs*); see Figure 10.13b. For each object, an ACL lists users and their permitted access rights. The ACL can contain a default, or public, entry. This allows users that are not explicitly listed as having special rights to have a default set of rights. The default set of rights should always follow the rule of least privilege or read-only access, whichever is applicable. Elements of the list include individual users as well as groups of users.

When it is desired to determine what access rights subjects have to a particular resource, ACLs are convenient because each ACL provides the information for a given resource. However, this data structure is not convenient for determining the access rights available to a specific user.

Decomposition by rows yields *capability tickets* (see Figure 10.13c). A capability ticket specifies authorized objects and operations for a particular user. Each user has a number of tickets and can be authorized to loan or give them to others. Because tickets can be dispersed around the system, they present a greater security problem than ACLs. The integrity of the ticket must be protected and guaranteed (usually by the operating system). In particular, the ticket must be unforgeable. One way to accomplish this is to have the operating system hold all tickets on behalf of users. These tickets have to be held in a region of memory that is inaccessible to users. Another alternative is to include an unforgeable token in the capability. This could be a large random password or a cryptographic message authentication code. This value is verified by the relevant resource whenever access is requested. This form of capability ticket is appropriate for use in a distributed environment, when the security of its contents cannot be guaranteed.

https://t.me/learningnets

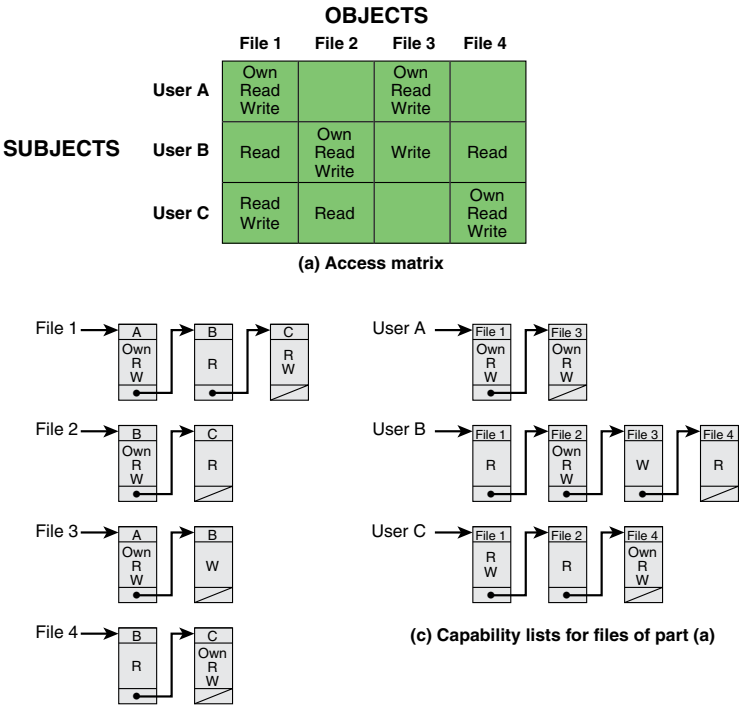


FIGURE 10.13 Examples of Access Control Structures

The convenient and inconvenient aspects of capability tickets are the opposite of those for ACLs. It is easy to determine the set of access rights that a given user has, but it is more difficult to determine the list of users with specific access rights for a specific resource.

Role-Based Access Control

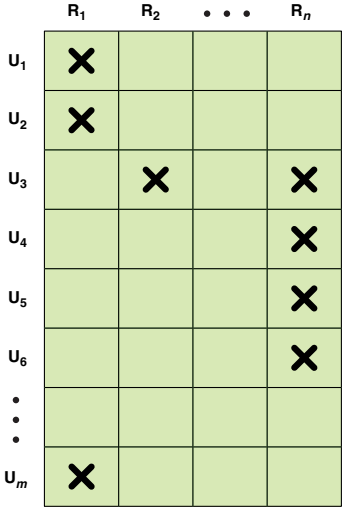
RBAC is based on the roles that users assume in a system rather than on the user's identity. Typically, RBAC models define a role as a job function within an organization. RBAC systems assign access rights to roles instead of individual users. In turn, users are assigned to different roles, either statically or dynamically, according to their responsibilities.

The relationship of users to roles is many to many, as is the relationship of roles to resources, or system objects. The set of users changes—in some environments frequently—and the assignment of a user to one or more roles may also be dynamic. The set of roles in the system in most environments is relatively static, with only

https://t.me/learningnets

occasional additions or deletions. Each role has specific access rights to one or more resources. The set of resources and the specific access rights associated with a particular role are also likely to change infrequently.

Use the access matrix representation to depict the key elements of an RBAC system in simple terms, as shown in Figure 10.14. The upper matrix relates individual users to roles. Typically, there are many more users than roles. Each matrix entry is either blank or marked, the latter indicating that this user is assigned to this role. Note that a single user may be assigned multiple roles (more than one mark in a row) and that multiple users may be assigned to a single role (more than one mark in a column). The lower matrix has the same structure as the DAC matrix, with roles as subjects. Typically, there are few roles and many objects, or resources. In this matrix, the entries are the specific access rights enjoyed by the roles. Note that a role can be treated as an object, allowing the definition of role hierarchies.



OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
• • •									
R_n			control		write	stop			

FIGURE 10.14 Access Control Matrix Representation of RBAC

https://t.me/learningnets

RBAC lends itself to effective implementation of the principle of least privilege. Each role should contain the minimum set of access rights needed for that role. A user is assigned to a role that enables him or her to perform only what is required for that role. Multiple users assigned to the same role, enjoy the same minimal set of access rights.

Attribute-Based Access Control

An ABAC model defines authorizations that express conditions on properties of both the resource and the subject. For example, consider a configuration in which each resource has an attribute that identifies the subject that created the resource. Then, a single access rule specifies the ownership privilege for all the creators of every resource. The strengths of the ABAC approach are its flexibility and expressive power.

Attributes are characteristics that define specific aspects of the subject, object, environment conditions, and/or requested operations that are predefined and preassigned by an authority. Attributes contain information that indicates the class of information given by the attribute, a name, and a value (for example, Class=HospitalRecordsAccess, Name=PatientInformationAccess, Value=MFBusinessHoursOnly).

The following are the three types of attributes in the ABAC model:

- **Subject attributes:** A subject is an active entity (for example, a user, an application, a process, or a device) that causes information to flow among objects or that changes the system state. Each subject has associated attributes that define the identity and characteristics of the subject. Such attributes include the subject's identifier, name, organization, job title, and so on. A subject's role is also viewed as an attribute.
- **Object attributes:** An object, also referred to as a *resource*, is a passive (in the context of the given request) information system–related entity (for example, devices, files, records, tables, processes, programs, networks, domains) containing or receiving information. As with subjects, objects have attributes that can be leveraged to make access control decisions. A Microsoft Word document, for example, has attributes such as title, subject, date, and author. Object attributes are often extracted from the metadata of the object. In particular, a variety of web service metadata attributes are relevant for access control purposes, such as ownership, service taxonomy, or even Quality of Service (QoS) attributes.
- **Environment attributes:** These attributes have so far been largely ignored in most access control policies. They describe the operational, technical, and even situational environment or context in which the information access occurs. For example, attributes such as current date and time, the current virus/hacker activities, and the network's security level (for example, Internet versus intranet) are not associated with a particular subject or a resource but may nonetheless be relevant in applying an access control policy.

https://t.me/learningnets

ABAC is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request. ABAC relies on the evaluation of attributes of the subject, attributes of the object, and a formal relationship or access control rule defining the allowable operations for subject/object attribute combinations in a given environment. All ABAC solutions contain these basic core capabilities to evaluate attributes and enforce rules or relationships between those attributes. ABAC systems are capable of enforcing DAC, RBAC, and MAC concepts. ABAC enables fine-grained access control, which allows for a larger number of discrete inputs into an access control decision, providing a bigger set of possible combinations of those variables to reflect a larger and more definitive set of possible rules, policies, or restrictions on access. Thus, ABAC allows an unlimited number of attributes to be combined to satisfy any access control rule. Moreover, ABAC systems can be implemented to satisfy a wide array of requirements from basic access control lists through advanced expressive policy models that fully leverage the flexibility of ABAC.

Figure 10.15 illustrates in a logical architecture the essential components of an ABAC system.

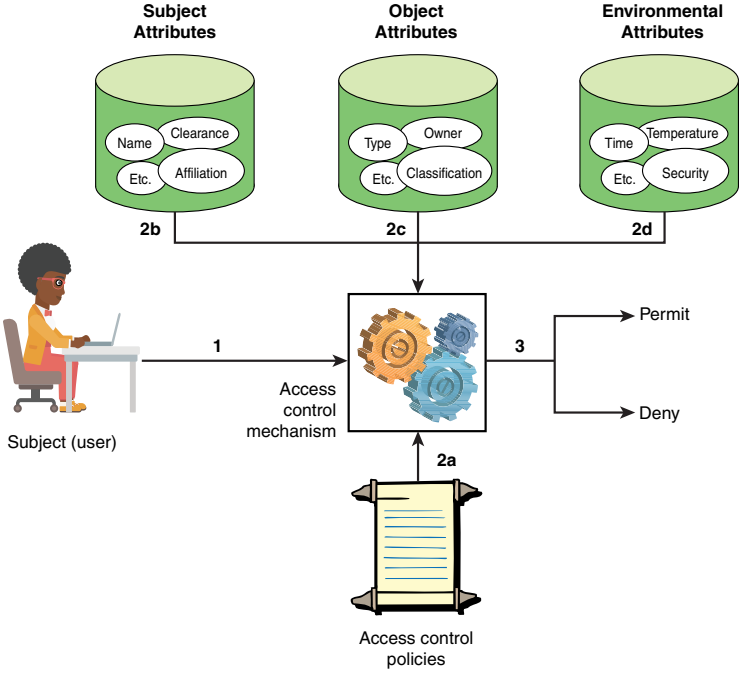


FIGURE 10.15 ABAC Scenario

https://t.me/learningnets

An access by a subject to an object proceeds according to the following steps:

1. A subject requests access to an object. This request is routed to an access control mechanism.
2. The access control mechanism is governed by a set of rules (2a) that are defined by a preconfigured access control policy. Based on these rules, the access control mechanism assesses the attributes of the subject (2b), object (2c), and current environmental conditions (2d) to determine authorization.
3. The access control mechanism grants the subject access to the object if access is authorized and denies access if it is not authorized.

It is clear from the logical architecture that there are four independent sources of information used for the access control decision. The system designer decides which attributes are important for access control with respect to subjects, objects, and environmental conditions. The system designer or other authority then defines access control policies, in the form of rules, for any desired combination of attributes of subject, object, and environmental conditions. This approach is very powerful and flexible. However, the cost, both in terms of the complexity of the design and implementation and in terms of the performance impact, is likely to exceed that of other access control approaches. This is a trade-off that the system authority must make.

Attribute Metadata

It is useful to have a standardized means of characterizing attributes and their values. The benefits include the following:

- Obtaining a better understanding of how the attribute and its value were obtained, determined, and vetted
- Having greater confidence in applying appropriate authorization decisions to subjects external to the domain of a protected system or data
- Developing more granular access control policies
- Making more effective authorization decisions
- Promoting the use of attributes across multiple organizations, such as in federated identity schemes, as discussed in Chapter 14

NISTIR 8112, *Attribute Metadata*, provides such a standardized method. The document includes metadata definitions for both attribute metadata and attribute value metadata. Attribute metadata are for the attribute itself, not for the specific attribute's value. For example, this metadata can describe the format in which the attribute is transmitted (for example, height is always recorded in inches). This schema provides a set of attribute

https://t.me/learningnets

metadata from which to choose when constructing an attribute sharing agreement (trust-time) and the rationale for their inclusion. The metadata items are:

- **Description:** An informative description of the attribute
- **Allowed values:** A defined set of allowed values for the attribute
- **Format:** A defined format in which the attribute is expressed
- **Verification frequency:** The frequency at which the attribute provider re-verifies the attribute

Attribute value metadata consists of elements that focus on the asserted value for the attribute. Following the same example as above, the attribute value is the actual height. A possible attribute value metadata for the height could be the name of the originating organization that provisioned the height (for example, the DMV in the subject's home state). The NISTIR 8112 schema provides a set of attribute value metadata, proposed values for those metadata fields, and rationale for their inclusion. The metadata fall into the following categories:

- **Provenance:** Metadata relevant or pertaining to evaluating the source of the attribute's value
- **Accuracy:** Metadata relevant or pertaining to determining if the attribute's value is correct and belongs to a specific subject
- **Currency:** Metadata relevant or pertaining to determining the "freshness" of a given attribute's value
- **Privacy:** Metadata relevant or pertaining to privacy aspects of a given attribute's value
- **Classification:** Metadata relevant or pertaining to the security classification of a given attribute's value

Table 10.6 provides details about the individual metadata items.

TABLE 10.6 Attribute Value Metadata

Metadata Element	Description	Recommended Values
Provenance		
Origin	The legal name of the entity that issues or creates the initial attribute value	■ Origin's name ■ None
Provider	The legal name of the entity that is providing the attribute	■ Provider's name ■ None

https://t.me/learningnets

Metadata Element	Description	Recommended Values
Pedigree	Description of the attribute value's relationship to the authoritative source of the value	■ Authoritative ■ Sourced ■ Self-asserted ■ Derived
Accuracy		
Verifier	The entity that verified the attribute's value	■ Origin ■ Provider ■ Not verified
Verification method	The method by which the attribute's value was verified as true and belonging to the specific individual	■ Document verification ■ Record verification ■ Document verification with record verification ■ Proof of possession ■ Not verified
Currency		
Last update	The date and time when the attribute was last updated	No restrictions
Expiration date	The date an attribute's value is considered to be no longer valid	No restrictions
Last verification	The date and time when the attribute's value was last verified as being true and belonging to the specified individual	No restrictions
Privacy		
Individual consented	Captures whether the user has expressly consented to providing the attribute's value	■ Yes ■ No ■ Unknown
Date consented	The date on which express consent for release of the attribute's value was acquired	No restrictions
Acceptable uses	Allowed uses for entities that receive attributes	■ Authorization ■ Secondary use ■ No further disclosure
Cache time to live	The length of time for which an attribute's value may be cached	No restrictions
Data deletion date	The date a certain attribute should be deleted from records	No restrictions
Classification		
Classification	Security classification level of the attribute	Enterprise specific
Releasability	Restrictions regarding to whom an attribute's value may be released	Enterprise specific

ABAC Resources

NIST has devoted considerable attention to ABAC. The following documents are useful for enterprises seeking to implement ABAC:

- **SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*:** A good introduction to ABAC, plus guidance for using ABAC

https://t.me/learninghets

to improve information sharing within organizations and between organizations while maintaining control of that information.

- **SP 800-178, *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications*:** Describes two different ABAC standards: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). The document compares them with respect to five criteria. The goal of this publication is to help ABAC users and vendors make informed decisions when addressing future data service policy enforcement requirements.
- **SP 1800-3, *Attribute Based Access Control*:** To assist enterprises interested in deploying ABAC, this publication develops an example of an advanced access control system. This ABAC solution manages access to networked resources more securely and efficiently and with greater granularity that traditional access management. It enables the appropriate permissions and limitations for the same information system for each user based on individual attributes and allows for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden. The approach uses commercially available products that are included alongside an enterprise's current products in their existing infrastructure. This example solution is packaged as a "how-to" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world. It saves organizations research and proof-of-concept costs for mitigating risk through the use of context for access decisions.
- **NISTIR 8112, *Attribute Metadata*:** Describes a schema for attribute metadata and attribute value metadata intended to convey information about a subject's attribute(s).

Access Control Metrics

Regardless of which access control scheme an enterprise uses, there is considerable complexity involved, and the organization needs to evaluate the effectiveness of the access control system. NISTIR 7874, *Guidelines for Access Control System Evaluation Metrics*, discusses a number of metrics that are used in access control evaluation, divided into four categories:

- **Administration:** Properties that in general impact the cost, efficiency, and performance of an access control system's administration.
- **Enforcement:** Properties of the mechanisms or algorithms that the access control system uses to enforce the embedded access control models and rules. These properties affect the efficiency of rendering access control decisions.
- **Performance:** Properties that impact performance in addition to the enforcement of the access control system's processes.

https://t.me/learningnets

- **Support:** Properties that are not essential but increase the usability and portability of an access control system.

Table 10.7 lists the individual metrics in each category.

TABLE 10.7 Evaluation Metrics for Access Control Systems

Administrative Properties	Enforcement Properties
Auditing Privileges/capabilities discovery Ease of privilege assignments Syntactic and semantic support for specifying AC rules Policy management Delegation of administrative capabilities Flexibilities of configuration into existing systems The horizontal scope (across platforms and applications) of control The vertical scope (between application, DBMS, and OS) of control	Policy combination, composition, and constraint Bypass Least privilege principle support Separation of Duty (SoD) Safety (confinements and constraints) Conflict resolution or prevention Operational/situational awareness Granularity of control Expression (policy/model) properties Adaptable to the implementation and evolution of AC policies
Support Properties	**Performance Properties**
Policy import and export OS compatibility Policy source management User interfaces and API Verification and compliance function support	Response time Policy repository and retrieval Policy distribution Integrated with authentication function

For each metric, NISTIR 7874 lists a number of questions to be used in evaluation. For example, the auditing metric includes the following questions:

- Does the access control system log system failure? The log for the source of errors records when the access control system fails to make grant decisions.
- Does the access control system log denied access requests? The log for the attempted policy violations records the denied user requests with respect to the access control policies involved.
- Does the access control system log granted access requests? The log for the access tracking records the granted capabilities of a subject. Because objects can be renamed, copied, and given away, tracking the dissemination and retention of access is difficult or impossible to achieve through privilege expressions alone.
- Does the access control system provide additional log functions required by the organization? It is possible to customize the audit information-providing capabilities for managing log data (for example, set the maximum size of audit logs).

https://t.me/learningnets

Trade-offs and limitations are involved with all access control mechanisms when considering the selection of properties, so it is the organization's responsibility to determine the best-fit access control metrics (thus, mechanisms) that work for the specific business functions and requirements. Proper selection of metrics depends not only on the consideration of administration cost but also on the flexibility of the mechanism used.

10.8 Customer Access

Customer access refers to access to business applications by individuals (for example, a purchaser placing orders for goods on a website, users of online banking or representatives of an organization gaining access on behalf of a corporation). Customer access presents additional considerations and security challenges beyond those involved with system access for employees. For example, as a general rule, customers do not receive security awareness training or training in the use and enforcement of security policy normally provided to employees.

This section organizes these considerations into four topics: customer access arrangements, customer contracts, customer connections, and protecting customer data.

Customer Access Arrangements

Many of the security controls implemented to provide security for employee access to business applications apply to customers as well. However, management needs to determine that in each individual case these controls are applied to ensure that all aspects of customer access to the organization's business applications meet security requirements.

Prior to providing customers with access to specific applications and information resources, a risk assessment must be carried out and the required controls identified. An individual or a group within the organization should be given responsibility for authorizing each customer access arrangement. In addition, each customer needs to be uniquely identified and approved by the owner of the application, who designates the access privileges for this customer.

If it is appropriate, provide the customer with awareness training and education relevant to the threats associated with customer access and the possible consequences in the event access is compromised.

Consult various stakeholders within the organization to determine the appropriate balance between providing for customer satisfaction and convenience on the one hand and meeting security requirements on the other.

https://t.me/learningnets

Customer Contracts

Customers, of course, do not automatically have the legal and contractual obligations associated with employees, as discussed in Chapter 5, "People Management." It is therefore essential to have agreed, approved contracts between the organization and the customer that cover security arrangements. Key characteristics of the contract include:

- Assessed by an information security specialist
- Signed off by executive management (or equivalent)
- Reviewed on a regular basis (for example, annually)
- Retained by an appropriate business function (for example, the procurement or legal department)

Customer Connections

Customer access, whether provided on site or, more commonly, remotely over the Internet or on a private network, should be subject to the same types of technical controls discussed in earlier sections of this chapter. First, authorize each customer with the process defined in Section 10.1, which includes defining access privileges for applications, information, and other resources within the organization. Then, as with any user access to an application or other resources, determine the authentication assurance level and select an appropriate authentication procedure.

Protecting Customer Data

Just as an organization must implement measures to protect itself from security breaches of its data related to customer access, the organization is legally and ethically required to protect data about the customer, such as the information typically found in a customer account record. The customer account record is the basic unit of information about a customer. It holds critical data about a customer, including the standard data, such as name, order data, billing information, interaction information, and credit information. Today, companies are able to augment this customer record information with new forms of data, such as social media handles, comments from forums or blog post data, and profile information from social media platforms, such as Twitter, LinkedIn, and Facebook. Whether a more narrowly focused or a broader approach is taken to collecting and maintaining information about customers, a plan is needed for the protection of this information. This includes security controls for confidentiality, integrity, availability, and privacy.

https://t.me/learningnets

10.9 System Access Best Practices

The SGP breaks down the best practices in the System Access category into 2 areas and 10 topics and provides detailed checklists for each topic. The areas and topics are:

- **Access management:** The objective of this area is to restrict access to business applications, mobile devices, systems, and networks to authorized individuals for specific business purposes by requiring them to be granted access privileges in line with their role, authenticated using access control mechanisms (for example, password, token or biometric), and subject to a rigorous sign-on process before being provided with approved levels of access.
  - **Access control:** Lists the elements that should go into an access control policy, including considerations of methods of access control, limits based on the role or identity of the individual, and types of controls
  - **User authorization:** Indicates that a formal process be applied and documented for authorizing individuals to have access to resources.
  - **Access control mechanisms:** Discusses the need for performing risk assessment, determining access control requirements, and evaluating and selecting access control mechanisms.
  - **Access control mechanisms—password:** Outlines policies for creation, use, and management of passwords.
  - **Access control mechanisms—token:** Outlines policies for use of tokens.
  - **Access control mechanisms—biometric:** Outlines policies for use of biometrics.
  - **Sign-on process:** Defines policies for the sign-on process.
- **Customer access:** The objective of this area is to protect business applications that provide customer access by performing information risk assessments to determine information security requirements and implementing security arrangements that are supported by agreed, approved contracts.
  - **Customer access arrangements:** This topic focuses on access to business applications by individuals (for example, a purchaser placing orders for goods on a website, users of online banking or representatives of an organization gaining access on behalf of a corporation).
  - **Customer contracts:** Provides details of recommended contents of customer contracts to ensure that customers are legally and contractually bound to protect the organization's information, business applications, and systems and to ensure that the organization's security obligations are met.

https://t.me/learningnets

- **Customer connections:** Discusses policies and procedures to protect sensitive or critical information related to either the organization or the customer.

10.10 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

access control
applicant
attack surface
authentication
authentication factor
authentication assurance level (AAL)
authenticator
authorization
biometric
blacklist
claimant
connected hardware token
credential
credential service provider (CSP)
digital authentication
digital identity
disconnected hardware token
electronic identity cards (eID)
false match rate (FMR)
false nonmatch rate (FNMR)
hardware token
identity proofing
inherence factor
knowledge factor
memory cards
multifactor authentication
offline dictionary attack
one-time password (OTP)
password
possession factor
rainbow table
relying party (RP)
salt
shadow password file
smart cards
subscriber
system access
user authentication
verifier

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. What does AAA mean in the context of system access?
2. What are the two main functions involved in user authentication?
3. Explain the three pillars of the NIST 800-63 digital identity model.
4. Name the entities and highlight their roles in NIST's digital identity model.
5. What are the three authentication factors in user identity authentication?
6. What are some typical attacks on password-based authentication? Enumerate countermeasures for each case.

https://t.me/learningnets

7. What purpose does the salt value serve with respect to a hashing function?
8. What are the major vulnerabilities of password file protection?
9. What are potential drawbacks of using a memory card as an authentication device?
10. How can you categorize authentication protocols used with a smart token?
11. What does OTP stand for, and what does it mean?
12. What are some likely threats to possession-based authentication?
13. What does *biometric authentication* mean?
14. What are some of the criteria used in designing a biometric system?
15. What does FMR stand for, and what does it mean?
16. What does PAD stand for, and what does it mean?
17. What does AAL stand for, and what does it mean?
18. How many levels are there for AAL?
19. What is out-of-band device authentication?
20. Describe customer access from an authentication point of view.

10.11 References

BONN12: Bonneau, J., "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords." *IEEE Symposium on Security and Privacy*, 2012.

BURN15: Burnett, M. "Today I Am Releasing Ten Million Passwords." February 9, 2015. https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495

GRAH12: Graham-Rowe, D., "Ageing Eyes Hinder Biometric Scans." *Nature*, May 2, 2012.

GOOD12: Goodin, D., "Why Passwords Have Never Been Weaker—and Crackers Have Never Been Stronger." *Ars Technica*, August 20, 2012.

HABI17: Habib, H., et al., "Password Creation in the Presence of Blacklists." *2017 Workshop on Usable Security*, 2017.

HERL12: Herley, C., & Oorschot, P., "A Research Agenda Acknowledging the Persistence of Passwords." *IEEE Security&Privacy*, January/February 2012.

https://t.me/learningnets

KELL12: Kelley, P., et al., "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms." *IEEE Symposium on Security and Privacy*, 2012

KOMA11: Komanduri, S., "Of Passwords and People: Measuring the Effect of Password-Composition Policies." *CHI Conference on Human Factors in Computing Systems*, 2011.

MAZU13: Mazurek, M., et al., "Measuring Password Guessability for an Entire University." *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, November 2013.

NIST15: NIST, *Measuring Strength of Authentication.* December 16, 2015. https://www.nist.gov/sites/default/files/nstic-strength-authentication-discussion-draft.pdf

NIST17: NIST, *Strength of Function for Authenticators—Biometrics (SOFA-B): Discussion Draft Open for Comments.* November 14, 2017. https://pages.nist.gov/SOFA/SOFA.html

NSTC11: National Science and Technology Council, *The National Biometrics Challenge.* September 2011.

OECH03: Oechslin, P., "Making a Faster Cryptanalytic Time-Memory Trade-Off." *Proceedings, Crypto 03*, 2003.

OPEN15: Openwall.com, *John the Ripper Password Cracker*. http://www.openwall.com/john/doc/

POLL12: Poller, A., et al., "Electronic Identity Cards for User Authentication—Promise and Practice." *IEEE Security & Privacy*, January/February 2012.

RATH01: Ratha, N., Connell, J., & Bolle, R., "Enhancing Security and Privacy in Biometrics-Based Authentication Systems." *IBM Systems Journal*, Vol 30, No 3, 2001.

TIMM10: Timmer, J., "32 Million Passwords Show Most Users Careless About Security." *Ars Technica*, January 21, 2010.

WAGN00: Wagner, D., & Goldberg, I., "Proofs of Security for the UNIX Password Hashing Algorithm." *Proceedings, ASIACRYPT '00*, 2000.

WEIR09: Weir, M., et al., "Password Cracking Using Probabilistic Context-Free Grammars." *IEEE Symposium on Security and Privacy*, 2009.

WEIR10: Weir, M., et al., "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords." *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 2010.

ZHAN10: Zhang, Y., Monrose, F., & Reiter, M., "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis." *ACM Conference on Computer and Communications Security*, 2010.

https://t.me/learningnets

Chapter 11

System Management

The function of a strong position is to make the forces holding it practically unassailable.

—*On War*, Carl Von Clausewitz

Learning Objectives

After studying this chapter, you should be able to:

- Summarize the main threats to server security.
- Distinguish between a type 1 hypervisor, a type 2 hypervisor, and containers.
- Distinguish between network attached storage and storage area networks.
- Summarize security considerations for network storage systems.
- Understand the use of service level agreements.
- Summarize the key concepts of performance and capacity management.
- Provide an overview of a backup policy.
- Understand the concepts involved in change management.
- Present an overview of system management best practices.

System management, or systems management, generally applied in the realm of information technology, is the enterprisewide management of IT systems and is usually directed by an organization's chief information officer (CIO). The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) divides this discipline into two main areas: system configuration and system maintenance (see Figure 11.1). Each of these areas is further divided into

https://t.me/learningnets

four topics. The first, computer and network installations, is covered in Chapter 12, "Networks and Communications." The remainder of the topics are discussed in this chapter.

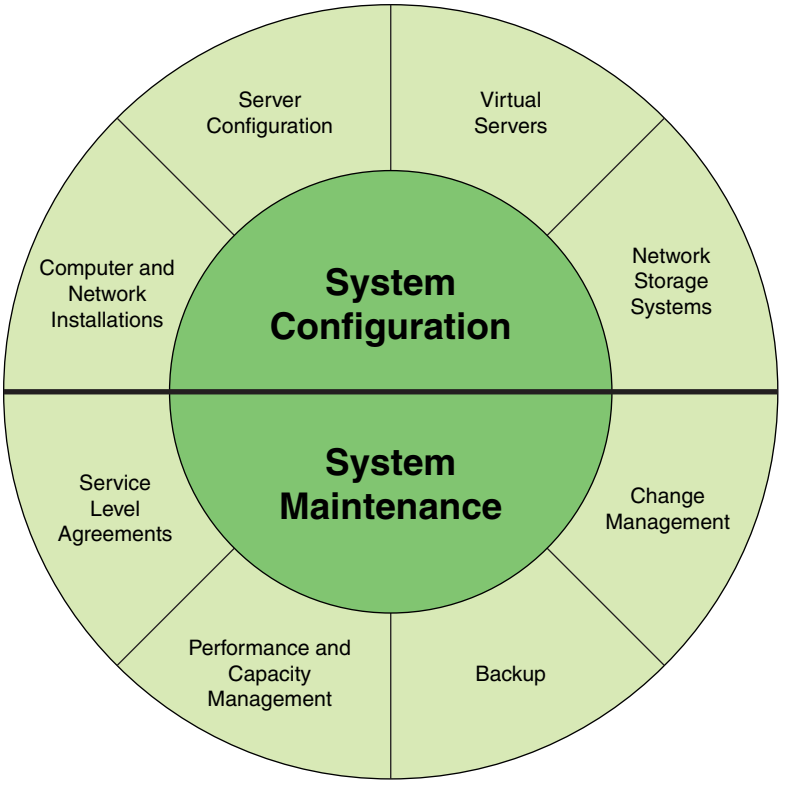


FIGURE 11.1 Elements of System Management

With respect to security, the objective of *system configuration* is to develop and enforce consistent system configuration policies that can cope with current and protected workloads and protect systems and the information they process and store against malfunction, cyber attack, unauthorized disclosure, and loss. Sections 11.1 through 11.3 address this area.

The objective of *system maintenance* is to provide guidelines for the management of the security of systems by performing backups of essential information and software, applying a rigorous change management process, and monitoring performance against agreed-upon service level agreements.

https://t.me/learningnets

11.1 Server Configuration

Servers are the heart of any enterprise IT facility. Servers host shared applications, shared data, and other shared resources. Servers provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for the organization. Some of the most common types of servers are application, web, email, database, infrastructure management, and file servers. This section addresses the general security issues of typical servers.

Threats to Servers

Server configuration needs to take into account the range of threats to server security that are possible or at least likely to exist. NIST SP 800-123, *Guide to General Server Security*, lists the following common security threats to servers:

- Malicious entities can exploit software bugs in the server or its underlying operating system, hypervisor, or containers to gain unauthorized access to the server.
- Denial-of-service (DoS) attacks can be directed to the server or its supporting network infrastructure, denying or hindering valid users from making use of its services.
- Sensitive information on the server can be read by unauthorized individuals or changed in an unauthorized manner.
- Sensitive information transmitted unencrypted or weakly encrypted between the server and the client can be intercepted. An example of weak encryption that is outdated but may still exist on legacy systems is single-stage Data Encryption Standard (DES).
- Malicious entities can gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the server.
- Malicious entities can attack other entities after compromising a server. These attacks can be launched directly (for example, from the compromised host against an external server) or indirectly (for example, placing malicious content on the compromised server that attempts to exploit vulnerabilities in the clients of users accessing the server). For many organizations, the majority of such attacks are internal (that is, from within the organization).

Requirements for Server Security

The following policy guidance is derived from a SANS Institute policy document template. The template defines some general requirements for server security as well as some specific configuration requirements.

https://t.me/learningnets

An enterprise should impose the following general requirements for server security:

- All internal servers deployed at the organization must be owned by an operational group that is responsible for system/server administration, including virtual servers.
- Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the chief information security officer (CISO).
- Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the CISO. The following items must be met:
  - Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location and a backup contact
    - Hardware and operating system/version
    - Main functions and applications, if applicable
  - Information in the corporate enterprise management system must be kept up-to-date.
  - Configuration changes for production servers must follow the appropriate change management procedures.



SANS Institute Information Security Policy Templates https://www.sans.org/security-resources/policies/

Specific configuration requirements include the following:

- Operating system configuration should be in accordance with approved security guidelines.
- Services and applications not used must be disabled where practical.
- Access to services should be logged and/or protected through access control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical; the only exception is when an application immediately interferes with business requirements.
- **Trust relationships** between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

trust relationship
A relationship between two different domains or areas of authority that makes it possible for users in one domain to be authenticated by a domain controller in the other domain.

https://t.me/learningnets

- Always use the standard security principle of least required access to perform a function. Do not use root when a non-privileged account suffices.
- If a methodology for secure channel connection is available (that is, technically feasible), perform privileged access over secure channels (for example, encrypted network connections using SSH or IPsec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

In addition, consider the following monitoring requirements:

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - Keep all security-related logs online for a minimum of one week.
  - Retain daily incremental tape backups for at least one month.
  - Retain weekly full tape backups of logs for at least one month.
  - Retain monthly full backups for a minimum of two years.
- Report security-related events to a security manager who reviews logs. Also report incidents to IT management. Prescribe corrective measures as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host

11.2 Virtual Servers

Virtualization refers to a technology that provides an abstraction of the computing resources used by some software, which thus runs in a simulated environment called a *virtual machine* (*VM*). Benefits arising from using virtualization include better efficiency in the use of the physical system resources than is typically seen using a single operating system instance. This is particularly evident in the provision of virtualized server systems. Virtualization also provides support for multiple distinct operating systems and associated applications on the one physical system. This is more commonly seen on client systems.

https://t.me/learningnets

Virtualization Alternatives

A *hypervisor* is software that sits between hardware and VMs and acts as a resource broker. It allows multiple VMs to safely coexist on a single physical server host and share that host's resources. The virtualizing software provides abstraction of all physical resources (such as processor, memory, network, and storage resources) and thus enables multiple computing stacks, called VMs, to be run on a single physical host.

Each VM includes an operating system, called the *guest operating system*. This operating system can be the same as the host operating system or a different one. For example, a guest Windows operating system could be run in a VM on top of a Linux host operating system. The guest operating system, in turn, supports a set of standard library functions and other binary files and applications. From the point of view of the applications and the user, this stack appears as an actual machine, with hardware and an operating system; thus, the term *virtual machine* is appropriate. In other words, it is the hardware that is virtualized.

A hypervisor performs the following functions:

- **Execution management of VMs:** This includes scheduling VMs for execution, virtual memory management to ensure VM isolation from other VMs, and context switching between various processor states. It also includes isolation of VMs to prevent conflicts in resource usage and emulation of timer and interrupt mechanisms.
- **Devices emulation and access control:** A hypervisor emulates all network and storage (block) devices that different native drivers in VMs are expecting, mediating access to physical devices by different VMs.
- **Execution of privileged operations by hypervisor for guest VMs:** Instead of being executed directly by the host hardware, certain operations invoked by guest operating systems, may have to be executed on its behalf by the hypervisor because of their privileged nature.
- **Management of VMs (also called VM life cycle management):** A hypervisor configures guest VMs and controls VM states (for example Start, Pause, Stop).
- **Administration of hypervisor platform and hypervisor software:** This involves setting parameters for user interactions with the hypervisor host as well as hypervisor software.

Type 1 and Type 2 Hypervisors

There are two types of hypervisors, distinguished by whether there is an operating system between the hypervisor and the host. A *type 1 hypervisor* (see Figure 11.2a) is loaded as a software layer directly onto a physical server, much as an operating system

https://t.me/learningnets

is loaded; this is referred to as *native virtualization*. The type 1 hypervisor directly controls the physical resources of the host. Once it is installed and configured, the server is then capable of supporting virtual machines as guests. In mature environments, where virtualization hosts are clustered together for increased availability and load balancing, a hypervisor can be staged on a new host. Then that new host is joined to an existing cluster, and VMs can be moved to the new host without any interruption of service.

Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

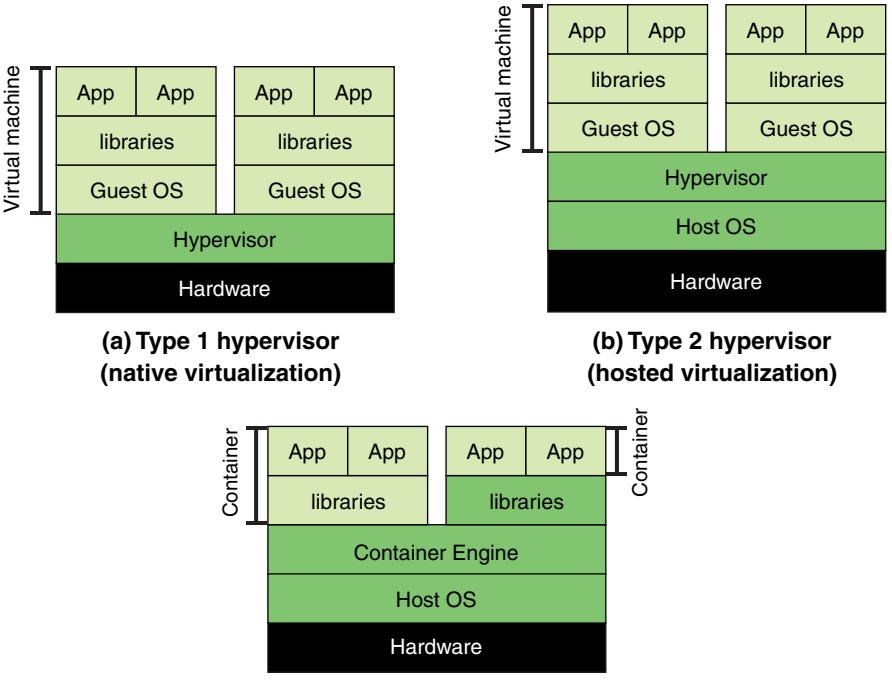


FIGURE 11.2 Comparison of Hypervisors and Containers

A *type 2 hypervisor* exploits the resources and functions of a host operating system and runs as a software module on top of the operating system (see Figure 11.2b); this is referred to as *hosted virtualization*, or *nested virtualization*. A type 2 hypervisor relies on the operating system to handle all the hardware interactions on the hypervisor's behalf.

https://t.me/learningnets

Key differences between the two hypervisor types are as follows:

- Typically, type 1 hypervisors perform better than type 2 hypervisors. Because a type 1 hypervisor doesn't compete for resources with an operating system, there are more resources available on the host, and, by extension, more virtual machines are hosted on a virtualization server using a type 1 hypervisor.
- Type 1 hypervisors are considered to be more secure than type 2 hypervisors. Virtual machines on a type 1 hypervisor make resource requests that are handled externally to that guest, and they cannot affect other VMs or the hypervisor that supports them. This is not necessarily true for VMs on a type 2 hypervisor, and a malicious guest could potentially affect more than itself.
- Type 2 hypervisors allow a user to take advantage of virtualization without needing to dedicate a server to only that function. Developers who need to run multiple environments as part of their process, in addition to taking advantage of the personal productive workspace that a PC operating system provides, can do both with a type 2 hypervisor installed as an application on their Linux or Windows desktop. The virtual machines that are created and used can be migrated or copied from one hypervisor environment to another, reducing deployment time and increasing the accuracy of what is deployed, reducing the time to market for a project.

Native virtualization systems, typically seen in servers, are used to improve the execution efficiency of the hardware. They are arguably also more secure, as they have fewer additional layers than the alternative hosted approach. Hosted virtualization systems are more common in clients, where they run at the same level as other applications on the host operating system, and are used to support applications for alternate operating system versions or types.

In virtualized systems, the available hardware resources—including include processor, memory, disk, network, and other attached devices—must be appropriately shared between the various guest operating systems. Processors and memory are generally partitioned between these operating systems and are scheduled as required. Disk storage can be partitioned, with each guest having exclusive use of some disk resources. Alternatively, a "virtual disk" can be created for each guest, which appears to the guest as a physical disk with a full file system but is viewed externally as a single "disk image" file on the underlying file-system. Attached devices such as optical disks or USB devices are generally allocated to a single guest operating system at a time. Several alternatives exist for providing network access. The guest operating system can have direct access to distinct network interface cards on the system; the hypervisor can mediate access to shared interfaces; or the hypervisor may implement virtual

https://t.me/learningnets

network interface cards for each guest, routing traffic between guests as required. This last approach is quite common and arguably the most efficient because traffic between guests does not need to be relayed via external network links. It does have security consequences in that this traffic is not subject to monitoring by probes attached to networks. Therefore, alternative, host-based probes are needed in such a system if such monitoring is required.

Some examples of type 2 hypervisors are VMware Workstation, Oracle VM Virtual Box, and Microsoft Windows Virtual PC.

Containers

A relatively recent approach to virtualization, known as *container virtualization* or *application virtualization*, is worth noting (refer to Figure 11.2c). In this approach, software known as a *virtualization container* runs on top of the host operating system kernel and provides an isolated execution environment for applications. Unlike hypervisor-based VMs, containers do not aim to emulate physical servers. Instead, all containerized applications on a host share a common operating system kernel. This eliminates the need for resources to run a separate operating system for each application and greatly reduces overhead.

For containers, only a small container engine is required as support for the containers. The container engine sets up each container as an isolated instance by requesting dedicated resources from the operating system for each container. Each container app then directly uses the resources of the host operating system. VM virtualization functions at the border of hardware and the operating system. It's able to provide strong performance isolation and security guarantees with the narrowed interface between VMs and hypervisors. The use of containers, which sit in between the operating system and applications, incurs lower overhead but potentially introduces greater security vulnerabilities.

Container technology is built into Linux in the form of Linux Containers (LXC). Other container capabilities include Docker, FreeBSD Jails, AIX Workload Partitions, and Solaris Containers. There are also container management systems that provide mechanisms for deploying, maintaining, and scaling containerized applications. Kubernetes and Docker Enterprise Edition are two examples of such systems.

Virtualization Security Issues

van Cleeff et al.'s "Security Implications of Virtualization: A Literature Study" [CLEE09], SP 800-125, *Guide to Security for Full Virtualization Technologies*,

https://t.me/learningnets

and SP 800-125A, *Security Recommendations for Hypervisor Deployment*, detail a number of security concerns that result from the use of virtualized systems, including the following:

- **Guest operating system isolation:** It is important to ensure that programs executing within a guest operating system can only access and use the resources allocated to it and cannot covertly interact with programs or data in either of the guest operating system's or in the hypervisor.
- **Guest operating system monitoring by the hypervisor:** The hypervisor has privileged access to the programs and data in each guest operating system and must be trusted as secure from subversion and compromised use of this access.
- **Virtualized environment security:** It is important to ensure security of the environment, particularly in regard to image and snapshot management, which attackers can attempt to view or modify.

These security concerns are regarded as an extension of the concerns already discussed with securing operating systems and applications. If a particular operating system and application configuration is vulnerable when running directly on hardware in some context, it is most likely also vulnerable when running in a virtualized environment. And if that system is actually compromised, it is capable of attacking other nearby systems, whether they are also executing directly on hardware or running as other guests in a virtualized environment. The use of a virtualized environment improves security by further isolating network traffic between guests than is the case when such systems run natively and from the ability of the hypervisor to transparently monitor activity on all guest operating systems. However, the presence of the virtualized environment and the hypervisor can reduce security if there are vulnerabilities in it that attackers can exploit. Such vulnerabilities allow programs executing in a guest to covertly access the hypervisor and, hence, other guest operating system resources. This problem, known as VM escape, is of concern. Virtualized systems also often provide support for suspending an executing guest operating system in a snapshot, saving that image, and then restarting execution at a later time, possibly even on another system. If an attacker views or modifies this image, the attacker compromises the security of the data and programs contained within it.

It is clear that the use of virtualization adds additional layers of concern, as previously noted. Securing virtualized systems means extending the security process to secure and harden these additional layers. In addition to securing each guest operating system and applications, an organization must secure the virtualized environment and the hypervisor.

https://t.me/learningnets

Securing Virtualization Systems

SP 800-125, which provides guidance for appropriate security in virtualized systems, states that organizations using virtualization should do the following:

- Plan the security of the virtualized system carefully.
- Secure all elements of a full virtualization solution, including the hypervisor, guest operating systems, and virtualized infrastructure—and also maintain their security
- Ensure that the hypervisor is properly secured
- Restrict and protect administrator access to the virtualization solution

Hypervisor Security

Secure the hypervisor by using a process similar to that with securing an operating system—that is, install it in an isolated environment, from known clean media, and update to the latest patch level in order to minimize the number of vulnerabilities present. The organization should then configure it so that it is updated automatically, disable or remove any unused services, disconnect unused hardware, use appropriate introspection capabilities with the guest operating systems, and monitor the hypervisor for any signs of compromise.

Limit access to the hypervisor to authorized administrators only, since these users are capable of accessing and monitoring activity in any of the guest operating systems. The hypervisor can support both local and remote administration. Configure appropriately, using suitable authentication and encryption mechanisms, particularly when using remote administration. Also consider remote administration access that is secured in the design of any network firewall and intrusion detection system (IDS) capability in use. Ideally such administration traffic should use a separate network, with very limited, if any, access provided from outside the organization.

Virtualized Infrastructure Security

Virtualized systems manage access to hardware resources such as disk storage and network interfaces. This access must be limited to just the appropriate guest operating systems that use any resource. As noted earlier, the configuration of network interfaces and use of an internal virtual network may present issues for organizations that wish to monitor all network traffic between systems. This should be designed and handled as needed.

Access to VM images and snapshots must be carefully controlled since these are another potential point of attack.

https://t.me/learningnets

Hosted Virtualization Security

Hosted virtualized systems, as typically used on client systems, pose some additional security concerns. These result from the presence of the host operating system under, and other host applications beside, the hypervisor and its guest operating systems. Hence, there are yet more layers to secure. Further, the users of such systems often have full access to configure the hypervisor and to any VM images and snapshots. In this case, the use of virtualization is more to provide additional features and to support multiple operating systems and applications than to isolate these systems and data from each other and from the users of these systems.

It is possible to design a host system and virtualization solution that is more protected from access and modification by the users. This approach can be used to support well-secured guest operating system images that provide access to enterprise networks and data and to support central administration and update of these images. However, there remain security concerns due to possible compromise of the underlying host operating system unless it is adequately secured and managed.

11.3 Network Storage Systems

Organizations make use of two broad categories of computer storage for files, databases, and other data: local and networked. Local storage, commonly called *direct access storage* (*DAS*), is a dedicated digital storage device attached directly to a server or PC via a cable or residing as an internal drive. Most users' computers and most servers have DAS. DAS creates data islands because data cannot be easily shared with other servers.

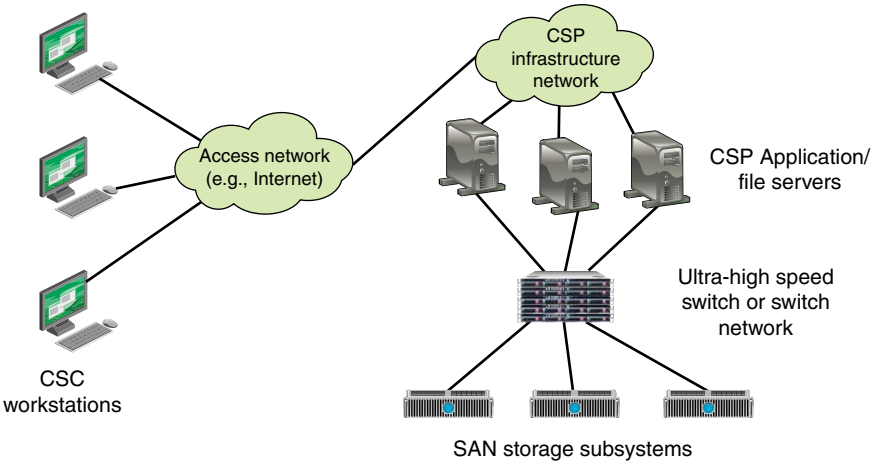
Networked storage is a term used to describe a storage device (usually many devices paired together) that is available over a network. This kind of storage maintains copies of data across high-speed local area network (LAN) connections and is designed to back up files, databases, and other data to a central location that can be easily accessed via standard network protocols and tools. Networked storage comes in the following topologies:

- **Storage area network (SAN):** A SAN is a dedicated network that provides access to various types of storage devices, including tape libraries, optical juke-boxes, and disk arrays. To servers and other devices in the network, a SAN's storage devices look like locally attached devices. A disk block–based storage technology, SAN is probably the most pervasive form of storage for very large data centers and is a de facto staple for database-intensive applications. These applications require shareable storage, large bandwidth, and support for the distances from rack to rack within the data center.

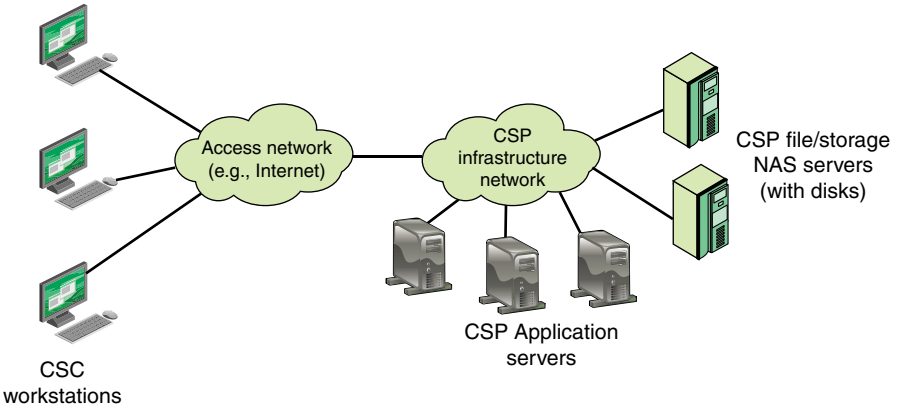
https://t.me/learningnets

- **Network attached storage (NAS):** NAS systems are networked appliances that contain one or more hard drives that are shared with multiple, heterogeneous computers. Their specialized role in networks is to store and serve files. NAS disk drives typically support built-in data protection mechanisms, including redundant storage containers or redundant arrays of independent disks (RAID). NAS enables file serving responsibilities to be separated from other servers on the network and typically provides faster data access than traditional file servers.

Figure 11.3 illustrates the distinction between SAN and NAS, using as an example cloud service customers (CSCs) connected to a cloud service provider (CSP).



(a) Configuration with storage area network (SAN)



(b) Configuration with network attached storage (NAS)

FIGURE 11.3 SAN and NAS in a Cloud Infrastructure

https://t.me/learningnets

The SGP recommends the following security measures:

- Follow the system development and configuration security policies for design and configuration of network storage systems.
- Be sure that SANs and NASs are subject to standard security practices (for example, configuration, malware protection, change management, patch management).
- Ensure that the IT facility provides protection of network storage management consoles and administration interfaces.
- Store encryption information on network storage systems.
- Allow for additional security arrangements specific to NAS and SAN.

Security arrangements specific to NAS and SAN depend on the type of server configuration, whether virtualization is used, and network configuration.

11.4 Service Level Agreements

A service level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider furnishes and defines the performance standards the provider is obligated to meet.

SLAs originated with network service providers but are now widely used in a range of IT-related fields. Companies that establish SLAs include IT service providers, **managed service providers (MSPs)**, and cloud computing service providers. Corporate IT organizations, particularly those that have embraced **IT service management (ITSM)**, enter SLAs with their in-house customers (users in other departments within the enterprise). An IT department creates an SLA so that its services can be measured, justified, and possibly even compared with those of outsourcing vendors.

A wide variety of SLAs are used in a number of contexts, each with its own typical metrics and service provisions. The following sections look at three important types of SLAs.

managed service provider (MSP)
A company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.

IT service management (ITSM)
A general term that describes a strategic approach for designing, delivering, managing, and improving the way IT is used in an organization. The goal of every ITSM framework is to ensure that the right processes, people, and technology are in place so that the organization can meet its business goals.

Network Providers

A network SLA is a contract between a network provider and a customer that defines specific aspects of the service to be provided. The definition is formal and typically defines quantitative thresholds that must be met. An SLA typically includes the following information:

- **A description of the nature of service to be provided:** A basic service is an IP-based network connectivity of enterprise locations plus access to the Internet. The service can include additional functions, such as web hosting, maintenance of domain name servers, and operation and maintenance tasks.

https://t.me/learningnets

- **The expected performance level of the service:** The SLA defines a number of metrics, such as delay, reliability, and availability, with numeric thresholds.
- **The process for monitoring and reporting the service level:** The SLA describes how performance levels are measured and reported.

Figure 11.4 shows a typical configuration that lends itself to an SLA. In this case, a network service provider maintains an IP-based network. A customer has a number of private networks (for example, LANs) at various sites. Customer networks are connected to the provider via access routers at the access points. The SLA dictates service and performance levels for traffic between access routers across the provider network. In addition, the provider network links to the Internet and thus provides Internet access for the enterprise.

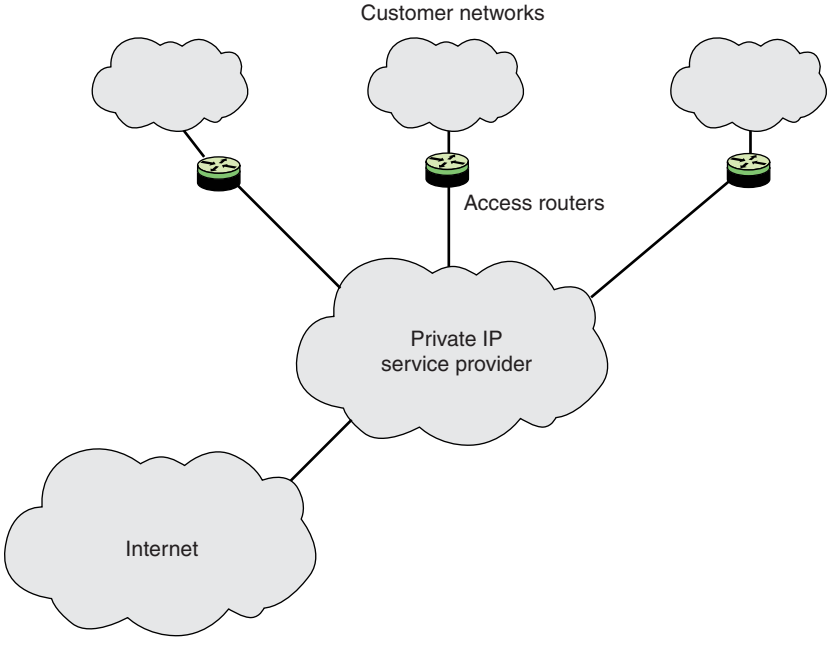


FIGURE 11.4 Typical Framework for a Service Level Agreement

For example, the standard SLA provided by Cogent Communications for its backbone networks includes the following items [COGE16]:

- **Availability:** 100% availability.
- **Latency (delay):** Monthly average network latency for packets carried over the Cogent network between backbone hubs for the following regions is as specified:

https://t.me/learningnets

- **Intra-North America:** 45 milliseconds or less
- **Intra-Europe:** 35 milliseconds or less
- **New York to London (transatlantic):** 85 milliseconds or less
- **Los Angeles to Tokyo (transpacific):** 125 milliseconds or less

Network latency (or round-trip time) is defined as the average time taken for an IP packet to make a round trip between backbone hubs within the regions specified above on the Cogent network. Cogent monitors aggregate latency within the Cogent network by monitoring round-trip times between a sample of backbone hubs on an ongoing basis.

- **Network packet delivery (reliability):** Average monthly packet loss no greater than 0.1% (or successful delivery of 99.9% of packets). Packet loss is defined as the percentage of packets that are dropped between backbone hubs on the Cogent network.

An SLA can be defined for the overall network service. In addition, SLAs are defined for specific end-to-end services available across the carrier's network, such as a virtual private network (VPN), or differentiated services.

Computer Security Incident Response Team

A computer security incident response team (CSIRT) is an organization that receives reports of security breaches, conducts analyses of the reports, and responds to the senders. An internal CSIRT is assembled as part of a parent organization, such as a government, a corporation, a university, or a research network. External CSIRTs provide paid services on either an ongoing or as-needed basis.

A computer security incident can involve a real or suspected breach or the act of willfully causing a vulnerability or breach. Typical incidents include the introduction of viruses or worms into a network, DoS attacks, unauthorized alteration of software or hardware, and identity theft of individuals or institutions. Hacking in general is considered a security incident unless the perpetrators were deliberately hired for the specific purpose of testing a computer or network for vulnerabilities; in that case, the hackers form part of the CSIRT, in a preventive role.

A CSIRT provides three main groups of services:

- **Reactive services (responses to incidents):** These are the main sources of work of a CSIRT
- **Proactive services:** Actions to prevent incidents from occurring in the future
- **Security quality management services:** Services that do not involve incidents but rather include working with IT or other organization departments in which CSIRT members help solidify security systems

https://t.me/learningnets

Response time is a critical consideration in assembling, maintaining, and deploying an effective CSIRT. A rapid, accurately targeted, and effective response minimizes the overall damage to finances, hardware, and software caused by a specific incident. Another important consideration involves the ability of the CSIRT to track down the perpetrators of an incident so that the guilty parties are shut down and effectively prosecuted. A third consideration involves hardening of the software and infrastructure to minimize the number of incidents that take place over time.

Table 11.1, from Carnegie Mellon University's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [CMU03], provides a representative list of service description attributes.

TABLE 11.1 CSIRT Service Description Attributes

Attribute	Description
Objective	Purpose and nature of the service.
Definition	Description of scope and depth of service.
Function descriptions	Descriptions of individual functions within the service.
Availability	The conditions under which the service is available: to whom, when, and how.
Quality assurance	Quality assurance parameters applicable for the service. Includes both setting and limiting of constituency expectations.
Interactions and information disclosure	The interactions between the CSIRT and parties affected by the service, such as the constituency, other teams, and the media. Includes setting information requirements for parties accessing the service and defining the strategy with regard to the disclosure of information (both restricted and public).
Interfaces with other services	Definition and specification of the information flow exchange points between this service and other CSIRT services it interacts with.
Priority	The relative priorities of functions within the service and of the service compared to other CSIRT services.

Cloud Service Providers

An SLA for a CSP includes security guarantees such as data confidentiality, integrity guarantees, and availability guarantees for cloud services and data. Roy et al.'s "Secure the Cloud: From the Perspective of a Service-Oriented Organization" [ROY15] lists the following considerations for a cloud provider SLA:

- Cloud storage needs to adhere to regulatory compliance laws of the region of data residency. This complicates matters for data confidentiality. For instance, CSPs may resort to hosting their cloud servers in countries that do not enable

https://t.me/learningnets

the government to subpoena CSPs into sharing client data from their servers, citing a threat to the nation as the reason. The existence of such laws in some countries puts data confidentiality at risk.

- Cloud storage SLAs should include strong proof of retrievability (PoR) guarantees; for instance, a cloud storage provider needs to provide strong metadata protection (that is, maintain freshness of data) as well as protection against loss (availability) or corruption (integrity) of data.
- Service unavailability (due to VM crash, for example) or data unavailability (data being nonretrievable) is caused by both security and nonsecurity issues. For instance, Amazon EC2 offers service availability with a guaranteed monthly uptime of 99.95% to the Infrastructure as a Service (IaaS) customer (no matter the cause of the downtime).
- Cloud network and front-end client applications must be secured against masquerading attackers (passive or active).
- Provision must also be made in the SLA to allow the client to audit security controls.

There may be differences in detail between public and private cloud SLAs, but fundamentally an organization requires the same sort of services in both cases.

11.5 Performance and Capacity Management

Performance and capacity management ensures that the IT capacity matches current and future needs of the business and that throughput and runtime requirements defined by the business are fulfilled. The critical success factors are:

- Understanding the current demands for IT resources and producing forecasts for future requirements
- Being able to plan and implement the appropriate IT capacity to match business needs and to demonstrate cost-effective interaction with other processes during the application life cycle

The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage, and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.

https://t.me/learningnets

Most organizations already collect some capacity-related information and work consistently to solve problems, plan changes, and implement new capacity and performance functionality. However, organizations do not routinely perform trending and what-if analyses. What-if analysis is the process of determining the effect of a network change. Trending is the process of performing baselines of network capacity and performance issues and reviewing the baselines for network trends to understand future upgrade requirements. Capacity and performance management should also include exception management, where problems are identified and resolved before users call in, and Quality of Service (QoS) management, where network administrators plan, manage, and identify individual service performance issues.

11.6 Backup

Backup is the process of making a copy of files and programs, to facilitate recovery, if necessary. The objective is to ensure the integrity and availability of information processed and stored within information processing facilities.

The following is a useful set of policies to ensure effective backup:

- Backups of all records and software must be retained such that computer operating systems and applications are fully recoverable. This is achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
- At least three versions of server data must be maintained.
- At a minimum, one fully recoverable version of all data must be stored in a secure offsite location. An offsite location can be in a secure space in a separate building or with an approved offsite storage vendor.
- Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
- An organization should store all data accessed from workstations, laptops, or other portable devices on networked file server drives to allow for backup. It should back up data located directly on workstations, laptops, or other portable devices to networked file server drives. Alternatively, data located directly on workstations, laptops, or other portable devices can be backed up using an approved third-party vendor. Convenience data and other information that does not constitute protected enterprise data do not carry this requirement.

https://t.me/learningnets

- Required backup documentation includes identification of all critical data, programs, documentation, and support items necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested annually.

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, recommends a strategy for backup and recovery that takes into account a risk assessment of the information to be stored and recovered, if necessary. Table 11.2 summarizes the strategy based on the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, security categories (low, moderate, and high).

TABLE 11.2 Backup and Recovery Guidelines

FIPS 199 Availability Impact Level	Information System Target Priority and Recovery	Backup/Recovery Strategy
Low	Low priority: Any outage with little impact, damage, or disruption to the organization	Backup: Tape backup Strategy: Relocate or cold site
Moderate	Important or moderate priority: Any system that, if disrupted, causes a moderate problem to the organization and possibly other networks or systems	Backup: Optical backup, WAN/VLAN replication Strategy: Cold
High	Mission-critical or high priority: Damage to or disruption of these systems causes the most impact on the organization, mission, and other networks and systems	Backup: Mirrored systems and disc replication

Three types of sites for backup are defined as alternatives:

- **Cold site:** A backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from the main computing location to an alternate site.

https://t.me/learningnets

- **Warm site:** An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.
- **Hot site:** A fully operational offsite data processing facility equipped with hardware and software to be used in the event of an information system disruption.

The alternate site choice must be cost-effective and match the availability needs of the organization's information systems. Thus, if a system requires near 100% availability, then a mirrored or hot site is the right choice. However, if the system allows for several days of downtime, then a cold site is a better option.

11.7 Change Management

COBIT 5 defines change management as a discipline which ensures that system software (operating systems and supporting applications), application software, and configuration files are introduced into production in an orderly and controlled manner. ISO 27002, *Code of Practice for Information Security Controls*, suggests the following items to be considered in implementing change management:

- Identification and recording of significant changes
- Planning and testing of changes
- Assessment of potential impacts, including information security impacts, of such changes
- Formal approval procedure for proposed changes
- Verification that information security requirements have been met
- Communication of change details to all relevant persons
- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events
- Provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident

Change management is critical for organizations and teams of various sizes and in various industries, including IT and manufacturing. It ensures that standardized methods, processes, and procedures are used for all changes, facilitate efficient and prompt handling of changes, and maintain the proper balance between the need for change and the potential detrimental impact it can cause.

https://t.me/learningnets

The following guidelines are useful in developing a change management strategy:

- **Communication:** Ensure that adequate advance notice of a change is given, especially if a response is expected. Provide clear guidance as to whom people should respond if they have comments or concerns.
- **Maintenance window:** A maintenance window is a period of time when maintenance, such as patching software or upgrading hardware components, is performed. Users should be alerted well in advance of any service disruptions.
- **Change committee:** This committee reviews change requests and determines whether they will be made. In addition, the committee may specify that certain changes to the proposed plan for implementing the change be made in order for it to be acceptable.
- **Critical changes:** An unscheduled change may be necessary to respond to a critical event. Even though some steps may need to be bypassed, as much consideration as possible is given to the possible consequences of attempting the change. It is still important to obtain sufficient approval for the change. What constitutes sufficient approval varies and should be defined by the department or business unit.
- **Plan the change:** The planning process is responsible for determining the following:
  - Who is responsible for the change
  - What effect the change will have
  - When the change should occur, based on the following factors:
    - When will the change have the least chance of interfering with operations?
    - Will appropriate support staff be available?
    - Can the change be made within the standard maintenance window?
    - Will there be enough time to review and test the proposed change?
  - Why making the change is important
  - How the change will be made
  - Whether the change results in any additional security issues or increases the risk to the system
  - Back-out procedures in case the change is not successful
  - What additional training and documentation are necessary for both support staff and end users

https://t.me/learningnets

- **Document change requests:** A change request form should be used to provide information about the change. A detailed form is appropriate for changes affecting data classified as confidential (highest, most sensitive), where protection is required by law, where the asset risk is high, and for information which provides access to physical or virtual resources. Table 11.3 describes the fields that comprise the change request form.

TABLE 11.3 Change Request Form Structure

Field	Description
Change Requested By	Enter the requester name and email address. If the request came from an external source, enter your name and the name of the external source.
Date of Change Request	Enter the date/time of the request.
Change Description	Enter a summary of the change required and a reason for the change.
Change Priority	Categorize the change request as urgent, high, medium, or low. If this change is time/date dependent, specify that here. Note that the change control committee may amend the priority/schedules depending on other activities.
Impact Assessment	Enter a summary of the business and technical functions that could be affected by these changes. Specify known risks and concerns in this section.
Pre-Deployment Test Plan	Describe how you will test the change before deployment. Note that testing changes greatly reduces the possibility of failures and unwanted surprises.
Back-Out Plan	Describe how a failed change can be backed out or how the resource can be restored to its previous state.
Post Deployment Test Plan	Describe how the change is tested to determine whether it was successful.
Change Approval	Specify whether the request was accepted or rejected. The change control committee should make this decision. If appropriate, a description of the decision should be included here.
Change Assignment	Specify the person responsible for implementing the change.

- **Test the change:** If a test environment is available, test the change prior to implementation.
- **Execute the change:** Include the following in the execution process:
  - Make sure support staff are available and prepared to assist in the change process.

https://t.me/learningnets

- If system availability is affected while the change is being made, notify affected individuals to let them know what to expect and when to expect it. They should also know who to contact if they experience difficulty as a result of the change.
- Verify that the change was successful and that the system is stable.
- Notify affected individuals that changes are complete.
- Provide documentation and instruction to users who will be affected by the change.
- Record that the change took place in the change log.

- **Keep a record of the change:** Keep a log or other record of all changes to supplement the change request document.

11.8 System Management Best Practices

The SGP breaks down the best practices in the System Management category into two areas and eight topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **System configuration:** The objective of this area is to develop and enforce consistent system configuration policies that can cope with current and protected workloads and protect systems and the information they process and store against malfunction, cyber attack, unauthorized disclosure, and loss.
  - **Computer and network installations:** Outlines the basic principles and practices for assuring that computer and network installations meet capacity/performance requirements and security requirements. Items covered include use of single sign-on, firewalls, traffic isolation, and capacity management.
  - **Server configuration:** Addresses issues related to security to take into account in server configuration.
  - **Virtual servers:** Addresses security issues related to the use of virtual servers.
  - **Network storage systems:** Provides a checklist for security issues related to various types of network storage.
- **System maintenance:** The objective of this area is to provide guidelines for the management of the security of systems by performing backups of essential information and software, applying a rigorous change management process, and monitoring performance against agreed service level agreements.

https://t.me/learningnets

- **Service level agreements (SLA):** Defines the business requirements for providers of any computer or network services, including those for information security, and to ensure that they are met.
- **Performance and capacity management:** Provides guidelines for ensuring adequate performance, capacity, and availability of systems and networks.
- **Backup:** Summarizes backup requirements and lists recommended measures for effective and secure backup.
- **Change management:** Provides guidance to ensure that changes are applied correctly and that they do not compromise the security of business applications, computer systems, or networks.

11.9 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

application virtualization
backup
cold site
computer security incident response team
container virtualization
direct attached storage (DAS)
hosted virtualization
hot site
hypervisor
IT service management (ITSM)
managed service provider (MSP)
native virtualization
network attached storage (NAS)
proactive service
reactive services
security quality management service
service level agreement (SLA)
storage area network (SAN)
system configuration
system maintenance
system management
trust relationship
type 1 hypervisor
type 2 hypervisor
virtual server
virtualization
virtualization container
network storage system
warm site

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Into how many areas does the SGP divide system management? Describe the areas.
2. According to NIST SP 800-123, what are some of the common security threats to servers?

https://t.me/learningnets

3. According to policy guidance from the SANS Institute, what are some general requirements for server security?
4. What does *virtualization* mean? What benefits does it offer to an organization?
5. What is a hypervisor? What functions does it perform?
6. What are the two types of hypervisors, based on presence of the operating system between hypervisor and the host?
7. What does *container virtualization* mean?
8. What are the three categories of network storage systems?
9. What does SLA stand for, and what does it mean? What are some common SLAs encountered in an IT organization?
10. How can an organization ensure effective backup?
11. What are the three types of sites for backup, according to FIPS 199?
12. List some useful guidelines for developing a change management strategy.

11.10 References

CLEE09: van Cleeff, A., Pieters, W., and Wieringa, R., "Security Implications of Virtualization: A Literature Study." *International Conference on Computational Science and Engineering*, IEEE, 2009.

CMU03: Carnegie Mellon University, *Handbook for Computer Security Incident Response Teams (CSIRTs).* CMU Handbook CMU/SEI-2004-HB-002, 2003.

COGE16: Cogent Communications, Inc., *Network Services Service Level Agreement Global*. September 2016. http://www.cogentco.com/files/docs/network/performance/global_sla.pdf

ROY15: Roy, A., et al., "Secure the Cloud: From the Perspective of a Service-Oriented Organization." *ACM Computing Surveys*, February 2015.

https://t.me/learningnets

Chapter 12

Networks and Communications

To guard against the baneful influence exerted by strangers is therefore an elementary dictate of savage prudence. Hence before strangers are allowed to enter a district, or at least before they are permitted to mingle freely with the inhabitants, certain ceremonies are often performed by the natives of the country for the purpose of disarming the strangers of their magical powers, or of disinfecting, so to speak, the tainted atmosphere by which they are supposed to be surrounded.

—*The Golden Bough*, Sir James George Frazer

Learning Objectives

After studying this chapter, you should be able to:

- List and define the key functions that a network management system should include.
- Give an overview of a network management system and explain each of its key components.
- Explain the role of firewalls as part of a computer and network security strategy.
- List the key characteristics of firewalls.
- Understand the security considerations for various aspects of network management.
- Understand the security considerations for various aspects of electronic communication.
- Present an overview of network and communications best practices.

This chapter provides a survey of security and security management issues related to two broad and related topics: networks and electronic communications. The chapter begins with an overview of network management concepts. Following this are sections covering firewalls and virtual private networks. With this background, the chapter then addresses the specific security concerns involved with network management. Next, the chapter examines electronic communications in the enterprise

https://t.me/learningnets

environment, including email, instant messaging, voice over IP networks, and telephony and conferencing.

12.1 Network Management Concepts

This section provides an overview of network management. Let's begin by looking at the requirements for network management. This will provide an idea of the scope of the task to be accomplished. To manage a network, it is fundamental to know something about the current status and behavior of that network.

Effective management requires a network management system that includes a comprehensive set of data gathering and control tools and that is integrated with the network hardware and software. Let's look at the general architecture of a network management system.

Network Management Functions

Table 12.1 lists key functions of network management, as suggested by the International Organization for Standardization (ISO) in ISO 7498-4, *Open Systems Interconnection—Basic Reference Model—Part 4: Management Framework*. A much more detailed description of these network management functions is contained in ITU-T (International Telecommunication Union Telecommunication Standardization Sector) M.3400, *Telecommunications Management Functions*. These categories provide a useful way of organizing this discussion of requirements.

TABLE 12.1 ISO Management Functional Areas

Category	Description
Fault management	The facilities that enable the detection, isolation, and correction of abnormal operation of the Open Systems Interconnection (OSI) environment
Accounting management	The facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects
Configuration management	The facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for continuous operation of interconnection services
Performance management	The facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities
Security management	The aspects of security essential to operate OSI network management correctly and to protect managed objects

https://t.me/learningnets

Fault Management

To maintain proper operation of a complex network, make sure that systems as a whole, as well as each essential component individually, are in proper working order. When a fault occurs, it is important to do the following as rapidly as possible:

- Determine exactly where the fault is
- Isolate the rest of the network from the failure so it continues to function without interference
- Reconfigure or modify the network in such a way as to minimize the impact of operation without the failed component or components
- Repair or replace the failed components to restore the network to its initial state

Central to the definition of fault management is the fundamental concept of a fault, as distinguished from an error. A *fault* is an abnormal condition that causes a device or system component to fail to perform in a required manner and that requires management attention (or action) for repair. A fault is usually indicated by failure to operate correctly or by excessive errors. For example, if a communications line is physically cut, no signals get through. Or a crimp in the cable can cause wild distortions so that there is a persistently high bit error rate. Certain errors (for example, a single bit error on a communication line) can occur occasionally and are not normally considered to be faults. It is usually possible to compensate for errors using the error control mechanisms of the various protocols.

Users expect fast and reliable problem resolution. Most end users tolerate occasional outages. When these infrequent outages do occur, however, users generally expect to receive immediate notification and expect the problem be corrected almost immediately. Providing such a level of fault resolution requires very rapid and reliable fault detection and diagnostic management functions. The impact and duration of faults are also minimized by the use of redundant components and alternate communication routes, to give the network a degree of fault tolerance. An organization should make sure the fault management capability is redundant to increase network reliability.

Users expect to be kept informed of the network status, including both scheduled and unscheduled disruptive maintenance. Users expect reassurance of correct network operation through mechanisms that use confidence tests or that analyze dumps, logs, alerts, or statistics. After correcting a fault and restoring a system to its full operational state, the fault management service must ensure that the problem is truly resolved and that no new problems are introduced. This requirement is called *problem tracking and control*.

https://t.me/learningnets

To satisfy requirements, fault management generally includes functions to do the following:

- Maintain and examine error logs
- Accept and act upon error detection notifications
- Trace and identify faults
- Carry out sequences of diagnostic tests
- Correct faults

As with other areas of network management, fault management should have minimal effect on network performance.

Accounting Management

In many enterprise networks, individual divisions or cost centers, or even individual project accounts, are charged for the use of network services. These are internal accounting procedures rather than actual cash transfers, but they are important to the participating users nevertheless. Furthermore, even if no such internal charging is employed, a network manager needs to be able to track the use of network resources by user or user class for a number of reasons, including the following:

- A user or group of users may abuse their access privileges and burden the network at the expense of other users.
- Users can make inefficient use of the network, and the network manager can assist in changing procedures to improve performance.
- The network manager is in a better position to plan for network growth if user activity is known in sufficient detail.

A network manager must specify the kinds of accounting information to be recorded at various nodes, the desired interval between successive transmissions of the recorded information to higher-level management nodes, and the algorithms used in calculating the charging.

To limit access to accounting information, the accounting facility must provide the capability to verify users' authorization to access and manipulate that information.

To satisfy requirements, accounting management generally includes functions to do the following:

- Inform users of costs incurred or resources consumed

https://t.me/learningnets

- Enable accounting limits to be set and tariff schedules to be associated with the use of resources
- Enable costs to be combined where multiple resources are invoked to achieve a given communication objective

Configuration Management

Modern data communication networks are composed of individual components and logical subsystems (for example, the device driver in an operating system) that are configured to perform many different applications. The same device, for example, can be configured to act either as a router or as an end system node or both. Once it is decided how a device is to be used, the configuration manager chooses the appropriate software and set of attributes and values (for example, a transport layer retransmission timer) for that device.

Configuration management is concerned with initializing a network and gracefully shutting down part or all of the network. It is also concerned with maintaining, adding, and updating the relationships among components and the status of components during network operation.

Startup and shutdown operations on a network are part of configuration management. It is often desirable for these operations on certain components to be performed unattended (for example, starting up or shutting down a network interface unit). A network manager needs to be able to identify initially the components that comprise the network and to define the desired connectivity of those components. Those who regularly configure a network with the same or a similar set of resource attributes need ways to define and modify default attributes and to load those predefined sets of attributes into the specified network components. A network manager needs to be able to change the connectivity of network components when users' needs change. Reconfiguration of a network is often desired in response to performance evaluation or in support of network upgrade, fault recovery, or security checks.

Users often need to, or want to, be informed of the status of network resources and components. Therefore, when changes in configuration occur, the network or system manager should notify users of these changes. The network or system manager should also generate configuration reports either on some routine periodic basis or in response to a request for such a report. Before reconfiguration, users often want to inquire about the upcoming status of resources and their attributes.

Network managers usually want only authorized users (operators) to manage and control network operation (for example, software distribution and updating).

https://t.me/learningnets

To satisfy requirements, configuration management generally includes functions to do the following:

- Set the parameters that control the routine operation of the system
- Associate names with managed objects and sets of managed objects
- Initialize and close down managed objects
- Collect information on demand about the current condition of the system
- Obtain announcements of significant changes in the condition of the system
- Change the configuration of the system

Performance Management

Modern data communications networks are composed of many and varied components, which must intercommunicate and share data and resources. In some cases, it is critical to the effectiveness of an application that the communication over the network be within certain performance limits. Performance management of a computer network comprises two broad functional categories: monitoring and controlling. Monitoring is the function that tracks activities on the network. The controlling function enables performance management to make adjustments to improve network performance. Some of the performance issues of concern to a network manager are as follows:

- What is the level of capacity utilization?
- Is there excessive traffic?
- Has throughput been reduced to unacceptable levels?
- Are there bottlenecks?
- Is response time increasing?

To deal with these concerns, a network manager must focus on some initial set of resources to be monitored to assess performance levels. This includes associating appropriate metrics and values with relevant network resources as indicators of different levels of performance. For example, what count of retransmissions on a transport connection is considered to be a performance problem requiring attention? Performance management, therefore, must monitor many resources to provide information in determining network operating level. By collecting this information, analyzing it, and then using the resultant analysis as feedback to the prescribed set of

https://t.me/learningnets

values, a network manager becomes more and more adept at recognizing situations that indicate present or impending performance degradation.

Before using a network for a particular application, a user may want to know such things as the average and worst-case response times and the reliability of network services. Thus, performance must be known in sufficient detail to respond to specific user queries. End users expect network services to be managed in such a way as to afford their applications consistently good response time.

Network managers need performance statistics to help them plan, manage, and maintain large networks. Performance statistics are used to recognize potential bottlenecks before they cause problems to end users. They also enable network managers to take appropriate corrective action. This action either takes the form of changing routing tables to balance or redistribute traffic load during times of peak use or when a bottleneck is identified by a rapidly growing load in one area. Over the long term, capacity planning based on such performance information indicates the proper decisions to make, for example, with regard to expansion of lines in that area.

To satisfy requirements, performance management generally includes functions to do the following:

- Gather statistical information
- Maintain and examine logs of system state histories
- Determine system performance under natural and artificial conditions
- Alter system modes of operation for the purpose of conducting performance management activities

Security Management

Security management is concerned with generating, distributing, and storing encryption keys. Passwords and other authorization or access control information must be maintained and distributed. Security management is also concerned with monitoring and controlling access to computer networks and access to all or part of the network management information obtained from the network nodes. Logs are an important security tool, and therefore security management is very much involved with the collection, storage, and examination of audit records and security logs, as well as with the enabling and disabling of these logging facilities.

Security management provides facilities for protection of network resources and user information. Network security facilities should be available for authorized users only.

https://t.me/learningnets

Users want to know that the proper security policies are in force and effective and that the management of security facilities is itself secure.

The purpose of security management is to support the application of security policies by means of functions that include the following:

- The creation, deletion, and control of security services and mechanisms
- The distribution of security-related information
- The reporting of security-related events

Network Management Systems

A large network cannot be put together and managed by human effort alone. The complexity of such a system dictates the use of automated network management tools. The urgency of the need for such tools is increased, and the difficulty of supplying such tools is also increased, if the network includes equipment from multiple vendors. Moreover, the increasing decentralization of network services, as exemplified by the increasing importance of workstations and client/server computing, makes coherent and coordinated network management increasingly difficult. In such complex information systems, many significant network assets are dispersed far from network management personnel.

Components of a Network Management System

A *network management system* is a collection of tools for network monitoring and control that is integrated in the following senses:

- A single operator interface with a powerful but user-friendly set of commands for performing most or all network management tasks
- A minimal amount of separate equipment, as most of the hardware and software required for network management is incorporated into the existing user equipment

A network management system consists of incremental hardware and software additions implemented among existing network components. The software used in accomplishing the network management tasks resides in the host computers and communications processors (for example, front-end processors, terminal cluster controllers, switches, routers). A network management system is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific attributes of each element and link known to the system. The active elements of the network provide regular feedback of status information to

https://t.me/learningnets

the network control center. In this context, the term element refers to network devices and end systems attached to the network.

Figure 12.1 suggests the principal components of a network management system. Each network node contains a collection of software devoted to the network management task, referred to in the diagram as a network management entity (NME).

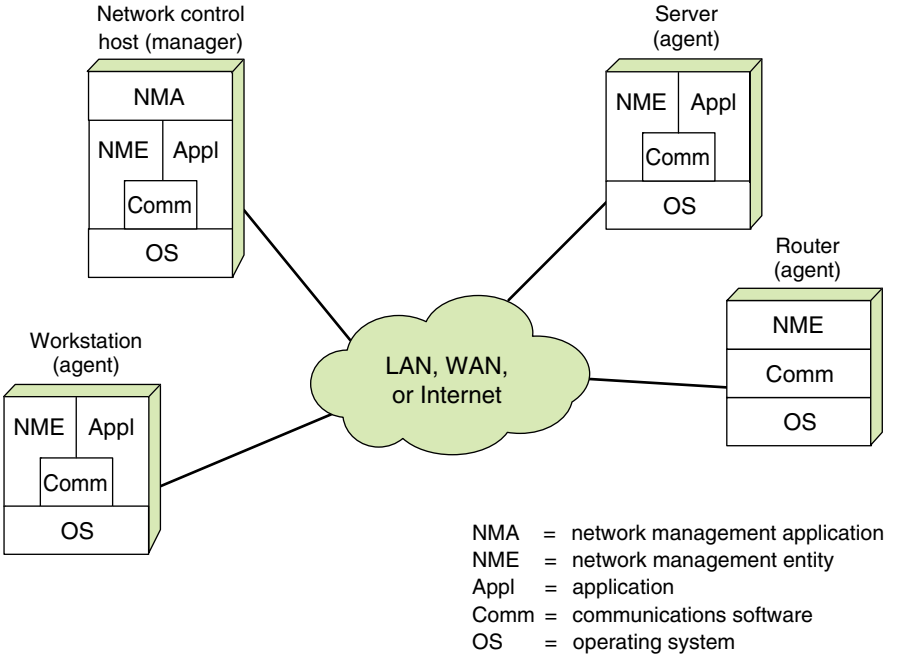


FIGURE 12.1 Components of a Network Management System

Each NME performs the following tasks:

- Collects statistics on communications and network-related activities
- Stores statistics locally
- Responds to commands from the network control center, including commands to do the following:
  - Transmit collected statistics to the network control center
  - Change a parameter (for example, a timer used in a transport protocol)

https://t.me/learningnets

- Provide status information (for example, parameter values, active links)
- Generate artificial traffic to perform a test

- Sends messages to the NCC when local conditions undergo significant changes

At least one host in the network is designated as the network control host, or *manager*. In addition to the NME software, the network control host includes a collection of software called the network management application (NMA). The NMA includes an operator interface to allow an authorized user to manage the network. The NMA responds to user commands by displaying information and/or by issuing commands to NMEs throughout the network. This communication is carried out using an application-level network management protocol that employs the communications architecture in the same fashion as any other distributed application.

Every other node in the network that is part of the network management system includes an NME and, for purposes of network management, is referred to as an *agent*. Agents include end systems that support user applications as well as nodes that provide a communications service, such as front-end processors, cluster controllers, bridges, and routers.

As depicted in Figure 12.1, the network control host communicates with and controls the NMEs in other systems. For maintaining high availability of the network management function, two or more network control hosts are used. In normal operation, one of the hosts is actively used for control, while the others are idle or simply collecting statistics. If the primary network control host fails, the backup system is used.

Distributed Network Management Systems

In a traditional centralized network management scheme, one host in the configuration has the role of a network management station; there can be one or two other management stations in a backup role. The remainder of the devices on the network contain agent software and a local database to allow monitoring and control from the management station. As networks grow in size and traffic load, such a centralized system is unworkable. Too much burden is placed on the management station, and there is too much traffic, with reports from every single agent having to wend their way across the entire network to headquarters. In such circumstances, a decentralized, distributed approach works best (see the example

https://t.me/learningnets

in Figure 12.2). In a decentralized network management scheme, there can be multiple top-level management stations, which are referred to as *management servers*. Each such server can directly manage a portion of the total pool of agents. However, for many of the agents, the management server delegates responsibility to an intermediate manager. The intermediate manager plays the role of manager to monitor and control the agents under its responsibility. It also plays an agent role to provide information and accept control from a higher-level management server. This type of arrangement spreads the processing burden and reduces total network traffic.

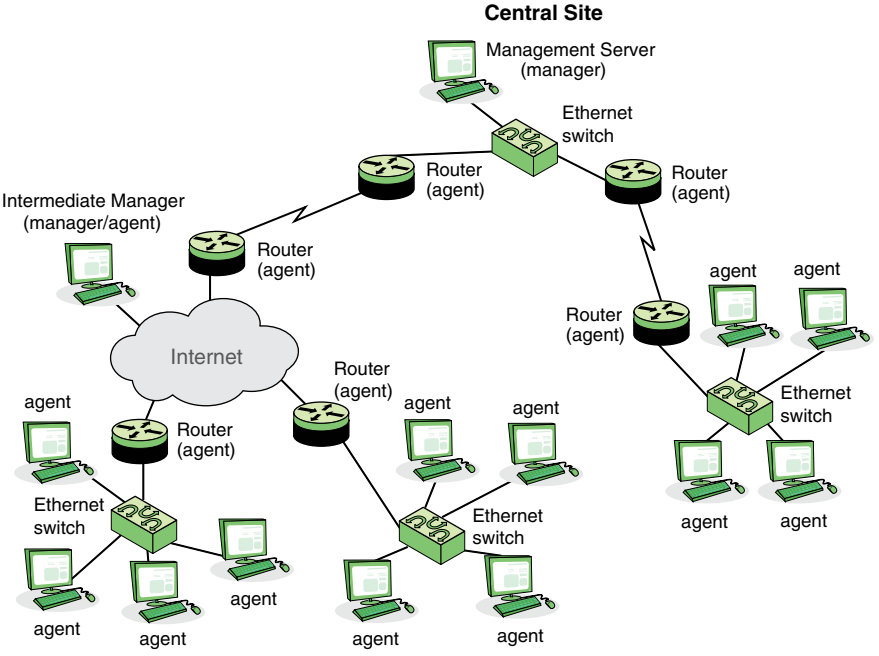


FIGURE 12.2 Example of a Distributed Network Management Configuration

Network Management Architecture

Cisco has developed a hierarchical network management architecture [CISC07] based on ITU M.3400, as shown in Figure 12.3.

https://t.me/learningnets

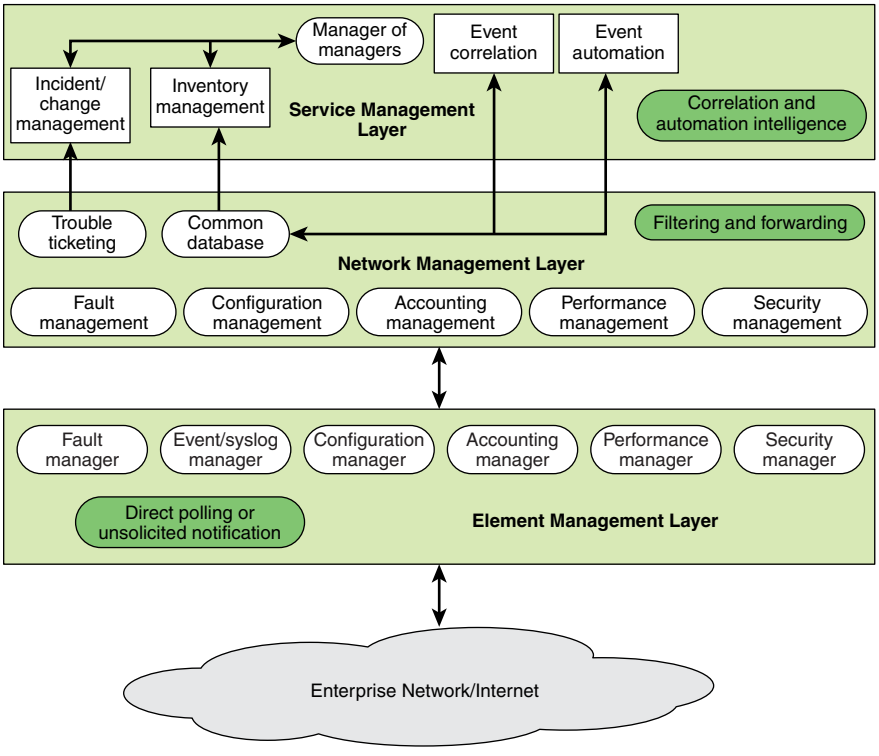


FIGURE 12.3 Network Management System Logical Architecture

The *element management layer* provides an interface to the network devices and communications links in order to monitor and control them. This layer captures events and fault occurrences through a combination of direct polling and unsolicited notification by network elements. Management function modules provide interfaces to specific elements, allowing elements from different manufacturers to be incorporated under a single network management system.

The *network management layer* (*NML*) provides a level of abstraction that does not depend on the details of specific elements. In terms of event management, this layer takes input from multiple elements (which in reality can be different applications), correlates the information received from the various sources (also referred to as root-cause analysis), and identifies the event that occurred. The NML provides a level of abstraction above the element management layer in that operations personnel are not "weeding" through potentially hundreds of unreachable or node down alerts but instead are focusing on the actual event, such as failure of an area-border router. Thus, this layer performs a filtering function, only providing a more aggregated view of

https://t.me/learningnets

the network through a common database across all five functions as well as a trouble ticketing facility.

The *service management layer* is responsible for adding intelligence and automation to filtered events, event correlation, and communication between databases and incident management systems. The goal is to move traditional network management environments and the operations personnel from element management (managing individual alerts) to network management (managing network events) to service management (managing identified problems).

12.2 Firewalls

The firewall is an important complement to host-based security services such as intrusion detection systems. Typically, a firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing are imposed. Firewalls are also deployed internally in an enterprise network to segregate portions of the network.

A firewall provides an additional layer of defense, insulating internal systems from external networks or other parts of the internal network. This follows the classic military doctrine of "defense in depth," which is applicable to IT security.

Firewall Characteristics

"Network Firewalls" [BELL94] lists the following design goals for a firewall:

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
- Only authorized traffic, as defined by the local security policy, is allowed to pass. Various types of firewalls are used, and they implement various types of security policies, as explained later in this chapter.
- The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

https://t.me/learningnets

In general terms, firewalls use four techniques that to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four techniques:

- **Service control:** Determines the types of Internet services that can be accessed—inbound or outbound. The firewall can filter traffic on the basis of IP address, protocol, or port number; provide proxy software that receives and interprets each service request before passing it on; or host the server software itself, such as a web or mail service.
- **Direction control:** Determines the direction in which particular service requests are initiated and allowed to flow through the firewall.
- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It can also be applied to incoming traffic from external users, though this requires some form of secure authentication technology, such as that provided in IP Security (IPsec).
- **Behavior control:** Controls how particular services are used. For example, the firewall can filter email to eliminate spam or enable external access to only a portion of the information on a local web server.

Before proceeding to the details of firewall types and configurations, let's consider the capabilities that are within the scope of a firewall:

- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection against various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
- A firewall provides a location for monitoring security-related events. Audits and alarms are implemented on the firewall system.
- A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function, which audits or logs Internet usage.
- A firewall serves as a platform for implementing virtual private networks (as discussed in the following section).

https://t.me/learningnets

Firewalls have limitations, including the following:

- A firewall cannot protect against attacks that bypass the firewall. Internal systems can have dial-out capability to connect to an ISP. An internal LAN can support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- A firewall does not fully protect against internal threats, such as disgruntled employees or employees who unwittingly cooperate with external attackers.
- An improperly secured wireless LAN can be accessed from outside the organization. An internal firewall that separates portions of an enterprise network does not guard against wireless communications between local systems on different sides of the internal firewall.
- A laptop, PDA, or portable storage device can be used and infected outside the corporate network and then attached and used internally.

Types of Firewalls

A firewall acts as a packet filter. It operates as a positive filter, allowing only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type, a firewall can examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. This section looks at the principal types of firewalls, shown in Figure 12.4.

Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing Internet Protocol (IP) packet and then forwards or discards the packet (see Figure 12.4b). This type of firewall is typically configured to filter packets going in both directions (from and to the internal network).

https://t.me/learningnets

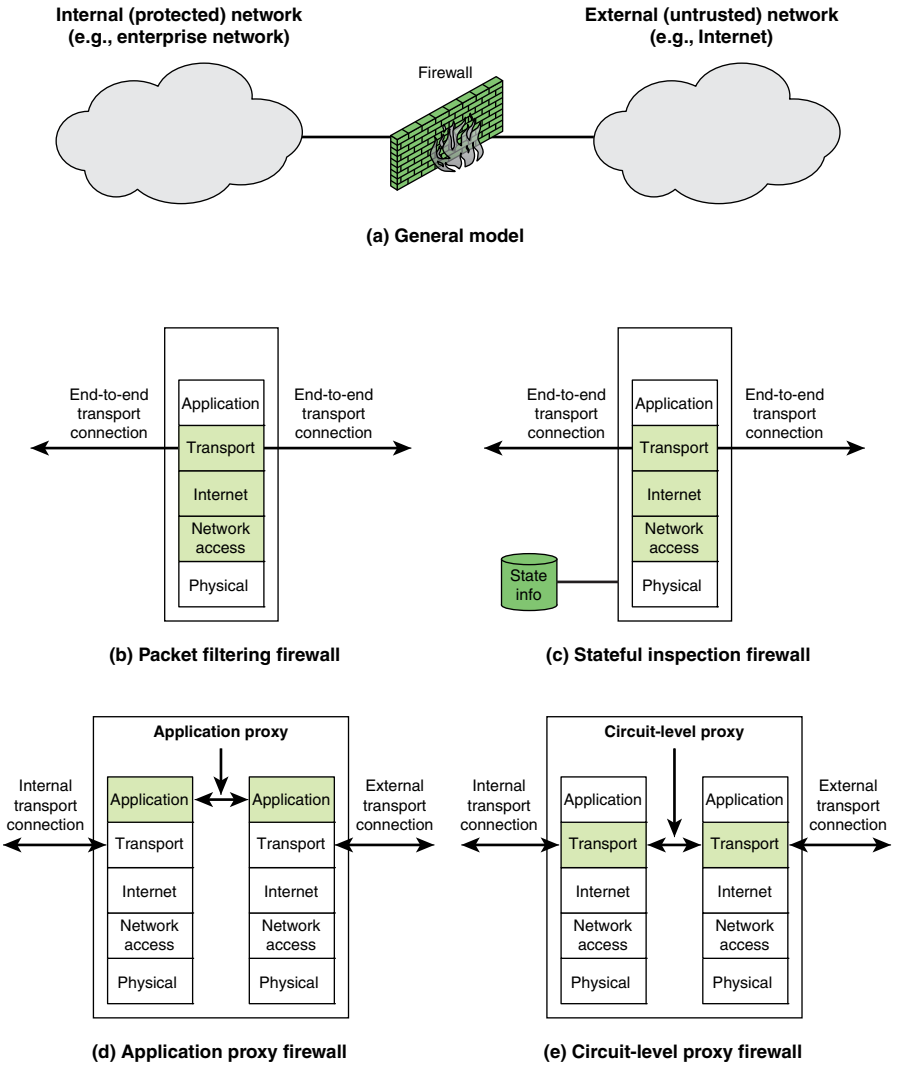


FIGURE 12.4 Types of Firewalls

Filtering rules are based on information contained in a network packet:

- **Source IP address:** The IP address of the system that originated the IP packet (for example, 192.178.1.1)
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (for example, 192.168.1.2)

https://t.me/learningnets

- **Source and destination transport-level addresses:** The transport-level (for example, Transmission Control Protocol [TCP] or User Datagram Protocol [UDP]) port number, which defines applications such as Simple Network Management Protocol (SNMP) or Telnet
- **IP protocol field:** The transport protocol
- **Interface:** For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for

A packet filter is typically set up as a list of rules, based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

- **Default = discard:** That which is not expressly permitted is prohibited.
- **Default = forward:** That which is not expressly prohibited is permitted.

The default = discard policy is the more conservative of the two. Initially, everything is blocked, and services are added on a case-by-case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. However, this is the policy likely to be preferred by businesses and government organizations. Further, visibility to users diminishes as rules are created. The default = forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence, react to each new security threat as it becomes known. This policy is used by generally more open organizations, such as universities.

Table 12.2 gives some examples of packet filtering rule sets. In each set, the rules are applied top to bottom. The * in a field is a wildcard designator that matches everything. Assume that the default = discard policy is in force with all these rule sets.

TABLE 12.2 Packet-Filtering Example

Rule Set A					
action	**ourhost**	**port**	**theirhost**	**port**	**comment**
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port
Rule Set B					
action	**ourhost**	**port**	**theirhost**	**Port**	**comment**
allow	*	*	*	25	connection to their SMTP port

https://t.me/learningnets

Rule Set C						
action	**src**	**port**	**dest**	**port**	**flags**	**comment**
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies
Rule Set D						
action	**src**	**port**	**dest**	**port**	**flags**	**comment**
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers
Rule Set E						
action	**ourhost**	**port**	**theirhost**	**Port**	**comment**	
block	*	*	*	*	default	

The rule sets can be described as follows:

- **Rule set A:** Inbound mail is allowed (port 25 is for Simple Mail Transfer Protocol [SMTP] incoming), but only to a gateway host. However, packets from a particular external host, SPIGOT, are blocked because that host has a history of sending massive files in email messages.
- **Rule set B:** This rule set is intended to specify that any inside host can send mail to the outside. A TCP packet with destination port 25 is routed to the SMTP server on the destination machine. The problem with this rule is that the use of port 25 for SMTP receipt is only a default; an outside machine can be configured to have some other application linked to port 25. As this rule is written, an attacker can gain access to internal machines by sending packets with TCP source port number 25.
- **Rule set C:** This rule set achieves the intended result that was not achieved in C. The rules take advantage of a feature of TCP connections. Once a connection is set up, the ACK flag of a TCP segment is set to acknowledge segments sent from the other side. Thus, this rule set states that it allows IP packets where the source IP address is one of a list of designated internal hosts and the destination TCP port number is 25. It also allows incoming packets with source port number 25 that include the ACK flag in the TCP segment. Note that you explicitly designate source and destination systems to define these rules.
- **Rule set D:** This rule set is one approach to handling File Transfer Protocol (FTP) connections. With FTP, two TCP connections are used: a control

https://t.me/learningnets

connection to set up the file transfer and a data connection for the actual file transfer. The data connection uses a different port number that is dynamically assigned for the transfer. Most servers, and hence most attack targets, use low-numbered ports; most outgoing calls tend to use a higher-numbered port, typically above 1023. Thus, this rule set allows:

- Packets that originate internally
- Reply packets to a connection initiated by an internal machine
- Packets destined for a high-numbered port on an internal machine

This scheme requires that the systems be configured so that only the appropriate port numbers are in use.

- **Rule set E:** This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule.

Rule set D points out the difficulty in dealing with applications at the packet filtering level. Another way to deal with FTP and similar applications is either to use stateful packet filters or an application-level gateway, both described subsequently in this section.

One advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast. However, packet filters have the following weaknesses:

- Because packet filtering firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, if a packet filtering firewall cannot block specific application commands and if a packet filtering firewall allows a given application, all functions available within that application are permitted.
- Because of the limited information available to the firewall, the logging functionality present in packet filtering firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- Most packet filtering firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality in the firewall.
- Packet filtering firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as *network layer address spoofing*. Many packet filtering firewalls cannot detect a network packet in which the OSI Layer 3 addressing information was altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.

https://t.me/learningnets

- Finally, due to the small number of variables used in access control decisions, packet filtering firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filtering firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.

Some of the attacks made on packet filtering firewalls and the appropriate countermeasures are as follows:

- **IP address spoofing:** The intruder transmits packets from the outside with a source IP address field containing an address of an internal host. The attacker hopes that the use of a spoofed address allows penetration of systems that employ simple source address security, in which packets from specific trusted internal hosts are accepted. The countermeasure is to discard packets with an inside source address if the packet arrives on an external interface. In fact, this countermeasure is often implemented at the router external to the firewall.
- **Source routing attacks:** The source station specifies the route for a packet to take as it crosses the Internet, in the hopes that this bypasses security measures that do not analyze the source routing information. The countermeasure is to discard all packets that use this option.
- **Tiny fragment attacks:** The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. This attack is designed to circumvent filtering rules that depend on TCP header information. Typically, a packet filter makes a filtering decision on the first fragment of a packet. All subsequent fragments of that packet are filtered out solely because they are part of the packet whose first fragment was rejected. The attacker hopes that the filtering firewall examines only the first fragment and that the remaining fragments are passed through. A tiny fragment attack is defeated by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header. If the first fragment is rejected, the filter remembers the packet and discards all subsequent fragments.

Stateful Inspection Firewalls

A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher-layer context. To understand what is meant by *context* and why a traditional packet filter is limited with regard to context, a little background is needed. Most standardized applications that run on top of TCP follow a client/server model. For example, for the SMTP, email is transmitted from

https://t.me/learningnets

a client system to a server system. The client system generates new email messages, typically from user input. The server system accepts incoming email messages and places them in the appropriate user mailboxes. SMTP operates by setting up a TCP connection between client and server, in which the TCP server port number, which identifies the SMTP server application, is 25. The TCP port number for the SMTP client is a number between 1024 and 65535 that is generated by the SMTP client.

In general, when an application that uses TCP creates a session with a remote host, it creates a TCP connection in which the TCP port number for the remote (server) application is a number less than 1024 and the TCP port number for the local (client) application is a number between 1024 and 65535. The numbers less than 1024 are the "well-known" port numbers and are assigned permanently to particular applications (for example, 25 for server SMTP). The numbers between 1024 and 65535 are generated dynamically and have temporary significance only for the lifetime of a TCP connection.

A simple packet filtering firewall must permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users.

A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 12.3. There is an entry for each currently established connection. The packet filter now allows incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

TABLE 12.3 Stateful Firewall Connection State Table Example

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.98.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

https://t.me/learningnets

A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall but also records information about TCP connections (refer to Figure 12.4c). Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. Some even inspect limited amounts of application data for some well-known protocols, such as FTP, instant messaging (IM), and Session Initiation Protocol (SIP) commands, in order to identify and track related connections.

Application-Level Gateway

An application-level gateway, also called an *application proxy*, acts as a relay of application-level traffic (refer to Figure 12.4d). The user contacts the gateway by using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and is not forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable, while denying all other features.

Application-level gateways are more secure than packet filters. Rather than try to deal with the numerous possible combinations that are allowed and forbidden at the TCP and IP levels, the application-level gateway only needs to scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level.

A prime disadvantage of this type of gateway is the additional processing overhead on each connection. In effect, there are two spliced connections between the end users, and the gateway, which is at the splice point, must examine and forward all traffic in both directions.

Circuit-Level Gateway

A fourth type of firewall is the circuit-level gateway, or *circuit-level proxy* (refer to Figure 12.4e). This is either a standalone system or a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one

https://t.me/learningnets

connection to the other without examining the contents. The security function consists of determining which connections are allowed.

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway is configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway incurs the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

Next-Generation Firewalls

Next-generation firewalls, which are implemented in either software or hardware, are capable of detecting and blocking complicated attacks by enforcing security measures at the protocol, port, and application levels. The difference between a standard firewall and a next-generation firewall is that the latter performs more in-depth inspection and in smarter ways. Next-generation firewalls also provide additional features such as Active Directory integration support, SSH (Secure Shell) and SSL (Secure Sockets Layer) inspection, and malware filtering based on reputation.

The common functionalities present in traditional firewalls—such as state inspection, virtual private networking, and packet filtering—are also present in next-generation firewalls. Next-generation firewalls are more capable of detecting application-specific attacks than standard firewalls and thus can prevent more malicious intrusions. Such a firewall does a full-packet inspection by checking the signatures and payload of packets for any anomalies or malware.

DMZ Networks

As shown in Figure 12.5, a firewall may be an internal or external firewall. An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or invite external connectivity, such as a corporate website, an email server, or a DNS (Domain Name System) server.

https://t.me/learningnets

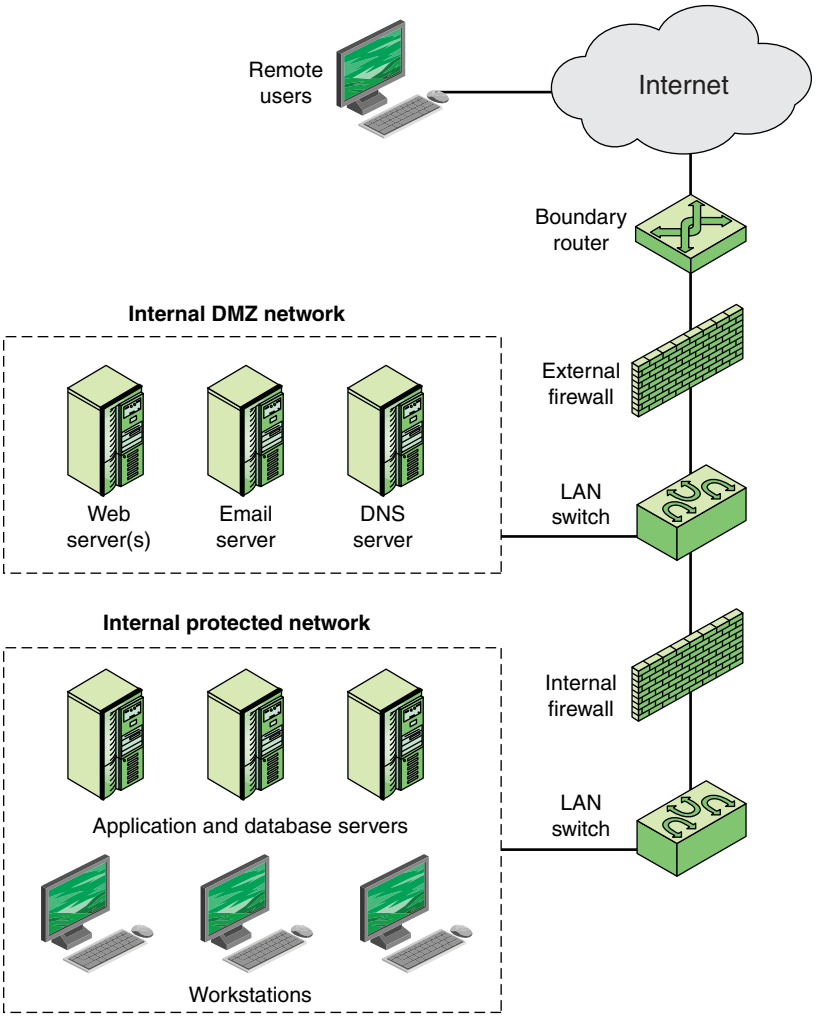


FIGURE 12.5 Firewall Configuration Example

An external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. An external firewall also provides a basic level of protection for the remainder of the enterprise network. In this type of configuration, internal firewalls serve three purposes:

- An internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.

https://t.me/learningnets

- An internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Second, an internal firewall protects the DMZ systems from attack from the internal protected network.
- Multiple internal firewalls are used to protect portions of the internal network from each other. For example, firewalls are configured so that internal servers are protected from internal workstations and vice versa. A common practice is to place the DMZ on a different network interface on the external firewall from that used to access the internal networks.

The Modern IT Perimeter

Traditionally, the enterprise network perimeter was defined by the physical interface between network devices, such as routers, and external networks, such as the Internet and private WANs. For today's enterprise, the perimeter is better defined by each node on the network and not the network itself. Key elements that break traditional network perimeter security are the following:

- **Wireless access points (APs):** Wi-Fi APs that are either unknowingly or maliciously deployed inside the enterprise network enable mobile devices on the premises or near the premises to gain access to resources on the enterprise network.
- **Mobile devices:** Mobile devices create a host of security issues, many of which are addressed in Chapter 7, "Physical Asset Management." One issue specifically related to perimeter control is the ability of a mobile device to connect to the Internet via the cellular network. This makes it possible for a computer in the enterprise network to connect to the mobile device and through that device to the Internet, without going through perimeter firewalls.

An IBM red paper [BUEC09] suggests that the following elements should comprise network perimeter defense in a wireless environment:

- The ability to globally enforce host-based security software deployed to the mobile systems known to access the enterprise network
- Scanning for, discovering, and blocking unknown devices

https://t.me/learningnets

- Monitoring traffic patterns, communications, and transmitted data to discover how the enterprise network is being used and to uncover unwanted or threatening traffic from mobile devices

12.3 Virtual Private Networks and IP Security

This section introduces the concept of virtual private networks and examines IPsec, a common security mechanism used with VPNs.

Virtual Private Networks

A *virtual private network* (*VPN*) is a private network that is configured within a public network (a carrier's network or the Internet) in order to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used by enterprises to create wide area networks that span large geographic areas, to provide site-to-site connections to branch offices, and to allow mobile users to dial up their company LANs. From the point of view of the provider, the pubic network facility is shared by many customers, and the traffic of each customer is segregated from other traffic. Traffic designated as VPN traffic can only go from a VPN source to a destination in the same VPN. It is often the case that encryption and authentication facilities are provided for the VPN.

In today's distributed computing environment, the VPN offers an attractive solution to network managers. In essence, a VPN consists of a set of computers that interconnect by means of a relatively insecure network and that make use of encryption and special protocols to provide security. At each corporate site, workstations, servers, and databases are linked by one or more LANs. The LANs are under the control of the network manager and are configured and tuned for cost-effective performance. The Internet or some other public network is used to interconnect sites, providing a cost savings over the use of a private network and offloading the WAN management task to the public network provider. That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites.

But the manager faces a fundamental requirement: security. Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, the manager can choose from a variety of encryption and authentication packages and products. Proprietary solutions raise a number of problems. First, how secure is the solution? If proprietary encryption or

https://t.me/learningnets

authentication schemes are used, there may be little reassurance in the technical literature about the level of security provided. Second is the question of compatibility. No manager wants to be limited in the choice of workstations, servers, routers, firewalls, and so on by a need for compatibility with the security facility. This is the motivation for the IPsec set of Internet standards.

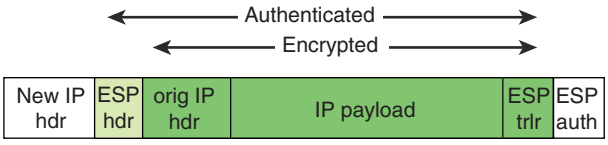
IPsec

IPsec is a set of Internet standards that augment both versions of IP that are in current use (IPv4 and IPv6) with security features. The principal feature of IPsec is that it encrypts and/or authenticates all traffic at the IP level. Thus, all distributed applications—including remote logon, client/server, email, file transfer, web access, and so on—are secured.

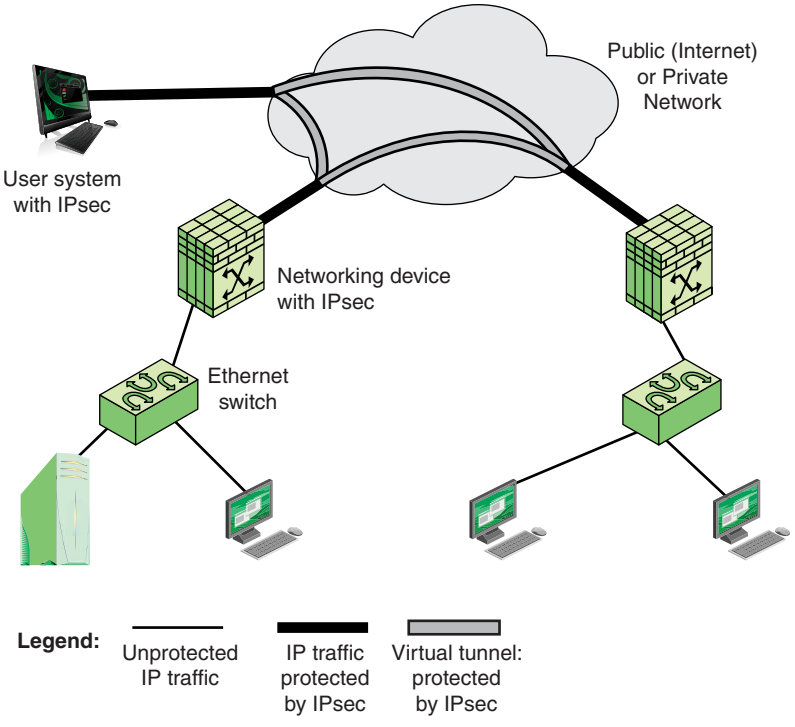
IPsec provides three main facilities: an authentication-only function referred to as Authentication Header (AH), a combined authentication/encryption function called Encapsulating Security Payload (ESP), and a key exchange function. For VPNs, both authentication and encryption are generally desired because it is important both to (1) ensure that unauthorized users do not penetrate the virtual private network and (2) ensure that eavesdroppers on the Internet cannot read messages sent over the VPN. Because both features are generally desirable, most implementations are likely to use ESP rather than AH. The key exchange function allows for manual exchange of keys as well as an automated scheme.

Figure 12.6a shows a simplified packet format for an IPsec option known as tunnel mode, using ESP and a key exchange function. Figure 12.6b shows a typical IPsec usage scenario. An organization maintains local area networks (LANs) at dispersed locations. Insecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPsec networking device typically encrypts and compresses all traffic going into the WAN and decrypts and decompresses traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial in to the WAN. Such user workstations must implement the IPsec protocols to provide security.

https://t.me/learningnets



(a) Tunnel-mode format



(b) Example configuration

FIGURE 12.6 An IPsec Tunnel Mode Scenario

Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet, including the security fields, is treated as the payload of new outer IP packet, with a new outer IP header. The entire original, inner, packet travels through a tunnel from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet can have totally different source and destination addresses, which increases the security. Tunnel mode is used

https://t.me/learningnets

when one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPsec. With tunnel mode, a number of hosts on networks behind firewalls can engage in secure communications without IPsec being implemented. The unprotected packets generated by such hosts are tunneled through external networks by tunnel mode SAs set up by the IPsec software in the firewall or secure router at the boundary of the local network.

Here is an example of how tunnel mode IPsec operates. Host A on a network generates an IP packet with the destination address of host B on another network. This packet is routed from the originating host to a firewall or secure router at the boundary of host A's network. The firewall filters all outgoing packets to determine the need for IPsec processing. If this packet from host A to host B requires IPsec, the firewall performs IPsec processing and encapsulates the packet with an outer IP header. The source IP address of this outer IP packet is this firewall, and the destination address can be a firewall that forms the boundary to B's local network. This packet is now routed to B's firewall, with intermediate routers examining only the outer IP header. At B's firewall, the outer IP header is stripped off, and the inner packet is delivered to B.

Firewall-Based VPNs

Figure 12.7 shows a typical scenario of IPsec usage. An organization maintains LANs at dispersed locations. Insecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPsec networking device typically encrypts and compresses all traffic going into the WAN and decrypts and decompresses traffic coming from the WAN; authentication can also be provided. These operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial in to the WAN. Such user workstations must implement the IPsec protocols to provide security. They must also implement high levels of host security, as they are directly connected to the wider Internet, which makes them an attractive target for attackers attempting to access the corporate network.

A logical means of implementing IPsec is in a firewall, as shown in Figure 12.8. If IPsec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted. In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses. IPsec can be implemented in the boundary router, outside the firewall. However, this device is likely to be less secure than the firewall and thus less desirable as an IPsec platform.

https://t.me/learningnets

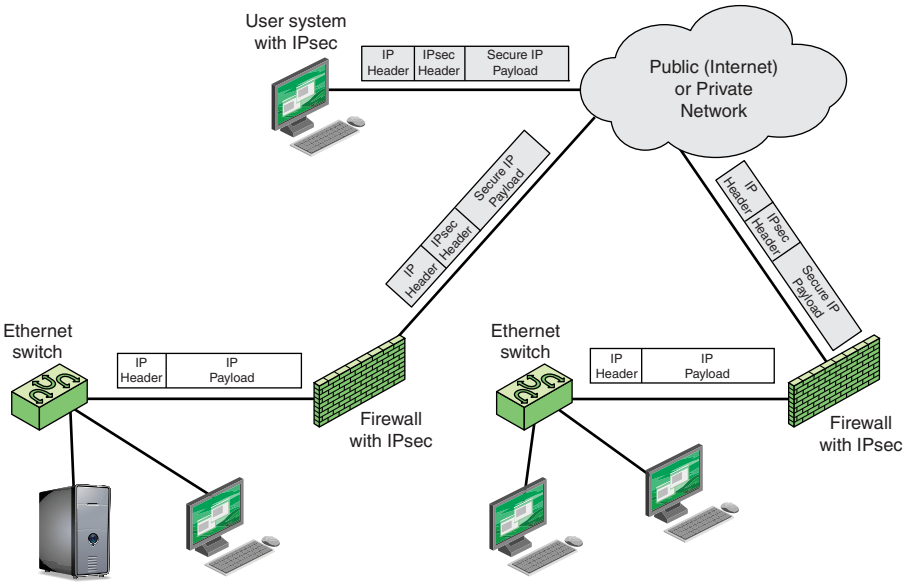


FIGURE 12.7 A VPN Security Scenario

12.4 Security Considerations for Network Management

This section addresses the network management topics defined in the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP).

Network Device Configuration

The principal security objective related to network device configuration is to ensure that the configuration of network devices is accurate and does not compromise the security of the network.

The SGP recommends that policies and procedures for device configuration cover:

- Security architecture principles
- Standard security management practices
- Device configuration
- Restriction of access to network devices
- Vulnerability and patch management

https://t.me/learningnets

- Changes to routing tables and settings in network devices
- Regular review of network device configuration and setup

Configuring network devices is a complex undertaking. As vendors build more features into their routers, switches, firewalls, and application delivery controllers, the command-line syntax required to configure those devices becomes increasingly loaded with options and syntactic choices. Web-based graphical user interfaces (GUIs) are often available as an alternative to a command-line interface (CLI), but they can be slow to navigate. Web GUIs also have a way of obfuscating functions by hiding them in unlikely pages, making accessing them require an annoying series of clicks.

Analyses by numerous IT experts have time and again revealed that the most common cause of network outages is faulty configuration changes [BANK14]. Even minor errors in configuration changes to the devices in production carry the risk of causing network outage. Therefore, skilled network administrators spend a significant part of their time configuring devices. They may find it hard to concentrate on strategic network engineering and administration tasks.

Most configuration changes are repetitive, labor-intensive tasks, such as changing passwords and access control lists. A number of tools and vendor offerings can automate repeatable and complex tasks related to device configuration, reducing the chance of human error. A Zoho Corp. white paper [BALA15] outlines the following important characteristics of automated network device configuration management tools:

- **Multivendor device support:** A tool should support all device types from all popular vendors.
- **Discovery capability for device addition:** A network can have thousands of network devices, and it is labor intensive to add each device manually. A tool should allow for discovering the devices in the network and automatically adding them, in addition to other device addition options.
- **Communication protocols:** A tool should support a wide range of protocols for establishing communication with the device and transferring configuration files.
- **Secure storage:** A tool should store configuration data in encrypted form, protected against intrusion.
- **Inventory:** A tool should provide an informative inventory of the devices being managed. It should provide various details, such as serial numbers, interface details, chassis details, port configurations, IP addresses, and hardware properties of the devices.
- **Configuration operations and schedules:** A tool should provide simple, intuitive options in the GUI to carry out various configuration operations, such as

https://t.me/learningnets

retrieving, viewing, editing, and uploading configurations back to the device. It should include options to schedule the operations for automatic execution.

- **Configuration versioning:** A tool should associate a version number with the configuration of each device, incremented with each change.
- **Baseline configuration:** A tool should have a provision for labeling the trusted configuration version of each device as a baseline version to enable administrators to roll back a configuration to the baseline version in the event of a network outage.
- **Access control:** A tool should include an attribute-based or role-based access control scheme, as described in Chapter 14, "Technical Security Management," to provide security when multiple users have access to configuration tools.
- **Approval mechanism:** The security policies of many enterprises require certain types of changes carried out by certain levels of users to be reserved for review and approval by top administrators prior to the deployment of the changes.

Physical Network Management

Physical network management is one aspect of physical security, a topic explored in some detail in Chapter 16, "Local Environment Management." This section first lists some important aspects of physical network management and then introduces the TIA-492 infrastructure standard.

Network Aspects

Three aspects of physical network management are mentioned here:

- **Telecommunication cables:** Telecommunication cables both within a site and providing external access to a site need to be physically protected. This includes using armored conduit, locking inspection/termination points, and avoiding routes through publicly accessible areas.
- **Network access points:** It is important to store network access points in secure environments and make sure they are subject to physical security policies.
- **Network documentation:** It is important to clearly document network configuration and functionality.

TIA-492

The Telecommunications Industry Association (TIA) standard TIA-492, *Telecommunications Infrastructure Standard for Data Centers*, specifies the minimum requirements for telecommunications infrastructure of data centers.

https://t.me/learningnets

The standard specifies function areas and helps define equipment placement based on the standard hierarchical design for regular commercial spaces. This architecture anticipates growth and helps create an environment where applications and servers can be added and upgraded with minimal downtime. This standardized approach supports high availability and a uniform environment for implementing security measures. TIA-942 specifies that a data center should include functional areas, as shown in Figure 12.8.

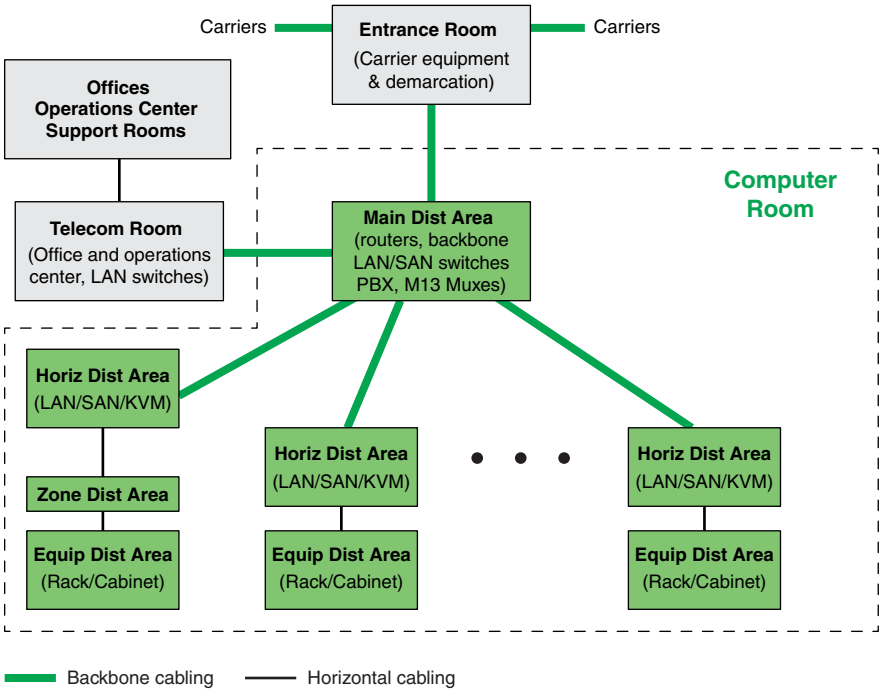


FIGURE 12.8 TIA-942-Compliant Data Center Showing Key Functional Areas

The functional areas are as follows:

- **Computer room:** This is the portion of the data center that houses data processing equipment.
- **Entrance room:** One or more entrance rooms house external network access provider equipment and provide the interface between the computer room equipment and the enterprise cabling systems. Physical separation of the entrance room from the computer room provides better security.

https://t.me/learningnets

- **Main distribution area:** This centrally located area houses the main cross-connect as well as core routers and switches for LAN and SAN (storage area network) infrastructures.
- **Horizontal distribution area (HDA):** The HAD serves as the distribution point for horizontal cabling and houses cross-connects and active equipment for distributing cable to the equipment distribution area.
- **Equipment distribution area (EDA):** The EDA is the location of equipment cabinets and racks, with horizontal cables terminating with patch panels.
- **Zone distribution area (ZDA):** The ZDA is an optional interconnection point in the horizontal cabling between the HDA and EDA. The ZDA acts as a consolidation point for reconfiguration flexibility or for housing freestanding equipment such as mainframes.

An important part of TIA-942 that is especially relevant for computer security is the concept of tiered reliability. The standard defines four tiers, as shown in Table 12.4. For each of the four tiers, TIA-942 describes detailed architectural, security, electrical, mechanical, and telecommunications recommendations such that the higher the tier, the higher the availability.

TABLE 12.4 Data Center Tiers Defined in TIA-942

Tier	System Design	Availability/Annual Downtime
1	■ This tier is susceptible to disruptions from both planned and unplanned activities. ■ There is a single path for power and cooling distribution with no redundant components. ■ It may or may not have a raised floor, a UPS, or a generator. ■ It takes 3 months to implement. ■ It must be shut down completely to perform preventive maintenance.	99.671%/ 28.8 hours
2	■ Tier 2 is less susceptible than tier 1 to disruptions from both planned and unplanned activity. ■ It has a single path for power and cooling distribution and includes redundant components. ■ It includes a raised floor, a UPS, and a generator. ■ It takes 3 to 6 months to implement. ■ Maintenance of the power path and other parts of the infrastructure requires a processing shutdown.	99.741%/ 22.0 hours

https://t.me/learningnets

Tier	System Design	Availability/Annual Downtime
3	■ Tier 3 enables planned activity without disrupting computer hardware operation, but unplanned events still cause disruption. ■ Multiple power and cooling distribution paths are available, though only one path is active; tier 3 includes redundant components. ■ It takes 15 to 20 months to implement. ■ It includes a raised floor and sufficient capacity and distribution to carry the load on one path while performing maintenance on the other.	99.982%/ 1.6 hours
4	■ Planned activity does not disrupt critical load and data center can sustain at least one worst-case unplanned event with no critical load impact ■ Multiple active power and cooling distribution paths, includes redundant components ■ Takes 15 to 20 months to implement	99.995%/ 0.4 hours

Wireless Access

The security aspects of network management for wireless access have the objective of ensuring that only authorized individuals and computing devices gain wireless access to networks and minimizing the risk of wireless transmissions being monitored, intercepted or modified.

Dennis Kennedy's article "Best Practices for Wireless Network Security" provides a useful list of risks associated with wireless access and mitigation techniques including the following:

- **Insufficient policies, training, and awareness:** As with other areas, wireless security controls must include policies and user awareness training specifically for wireless access. These include procedures regarding uses of wireless devices and an understanding of relevant risks.
- **Access constraints:** A wireless access point transmits, at regular intervals, a signal containing is Service Set Identifier (SSID). This unique SSID identifies the access point and is used to announce that the access point is active. Because SSIDs are transmitted unencrypted, an unauthorized use could exploit the SSID to attempt an attack or intrusion. Countermeasures include the following:
  - Enable device security features.
  - Change default settings, such as default SSIDs set by the manufacturer.
  - Use static IP addresses for wireless access points. This avoids the use of the Dynamic Host Configuration Protocol (DHCP), which automatically

https://t.me/learningnets

provides an IP address to anyone attempting to gain access to your wireless network. again Static IP addresses make unauthorized penetration more difficult.

- Track employees who have WLANs at home or at a remote site. Require that wireless networks be placed behind the main routed interface so the institution can shut them off if necessary. If WLANs are being used at home, require specific security configurations, including encryption and VPN tunneling.

- **Rogue access points:** Rogue access points are APs that users install without coordinating with IT. Access controls, encryption, and authentication procedures enable IT to maintain control.
- **Traffic analysis and eavesdropping:** To counter this threat, it is necessary to use a strong user authentication technique and to encrypt all traffic.
- **Insufficient network performance:** Poor performance is due to an imbalance in the use of access points, insufficient capacity planning, or a denial of service attack. The following steps can mitigate this risk.

  1. Continually monitor network performance and investigate any anomalies immediately.
  2. Segment the access point's coverage areas to reduce the number of people using each access point.
  3. Apply a traffic-shaping solution to allow administrators to proactively manage traffic rather than react to irregularities.

- **Hacker attacks:** Hackers attempt to gain unauthorized access over wireless networks. Intrusion detection systems, anti-virus software, and firewalls are mitigation techniques.
- **Physical security deficiencies:** This is in the domain of physical security. Subject Both the network devices and mobile devices to physical security policies and procedures.

Employ VPNs as an additional security control.

External Network Connections

The principal security objective with respect to external network connections is to prevent unauthorized external users from gaining access to information systems and networks. The SGP includes the following guidelines:

- Restrict external network traffic to only specified parts of information systems and networks and defined entry points.

https://t.me/learningnets

- Verify the sources of external connections.
- Limit access to devices that meet minimum security configuration requirements.
- Restrict access to only specific enterprise applications.
- Use firewalls to enforce security policies.
- Use a VPN for devices.

Firewalls

The security management of firewalls requires a clearly defined firewall policy that is compatible with an overall security policy and a plan for the implementation and operation of the organization's firewalls. The following subsections examine these two topics.

Firewall Policy

National Institute of Standards and Technology (NIST) SP 800-41, *Guidelines on Firewalls and Firewall Policy*, defines a *firewall policy* as a description of how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types, based on the organization's information security policies. SP 800-41 makes the following recommendations with respect to setting firewall policies:

- Base an organization's firewall policy on a comprehensive risk analysis.
- Base firewall policies on blocking all inbound and outbound traffic, with exceptions made for desired traffic.
- Take into account the source and destination of the traffic in addition to the content.
- By default, block many types of IPv4 traffic, such as traffic with invalid or private addresses.
- Have policies for handling incoming and outgoing IPv6 traffic.
- Determine which applications in the organization send traffic into or out of its network and make firewall policies to block traffic for other applications.

Firewall Planning and Implementation

With respect to planning and implementation, SP 800-41 offers the following advice on the phases involved:

- **Plan:** The first phase of the process involves identifying all requirements for an organization to consider when determining what firewall to implement to enforce the organization's security policy.

https://t.me/learningnets

- **Configure:** The second phase involves all facets of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system.
- **Test:** The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of testing are to evaluate the functionality, performance, scalability, and security of the solution and to identify any issues—such as interoperability—with components.
- **Deploy:** When testing is complete and all issues are resolved, the next phase focuses on deployment of the firewall into the enterprise.
- **Manage:** After the firewall has been deployed, it is managed throughout its life cycle, including component maintenance and support for operational issues. This life cycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

Remote Maintenance

Remote maintenance refers to maintenance activities conducted by individuals who are external to an information system's security perimeter. Remote maintenance is a convenience to the enterprise; in some environments it is a necessity, as an Internet of Things (IoT) deployment or an industrial control system. The principal security objective in this area is to prevent unauthorized access to critical systems and networks through the misuse of remote maintenance facilities.

The U.S. Department of Homeland Security has compiled a list of requirements for remote maintenance of industrial control system [DHS11], but this list has general applicability to IT systems as well. The requirements for an organization are as follows:

- Authorize, monitor, and control remotely executed maintenance and diagnostic activities.
- Allow the use of remote maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system.
- Maintain records for remote maintenance and diagnostic activities.
- Terminate all sessions and remote connections when remote maintenance is completed.
- If password-based authentication is used to accomplish remote maintenance, change passwords following each remote maintenance session.
- Audit remote maintenance and diagnostic sessions and ensure that designated organizational personnel review the maintenance records of the remote sessions.
- Document the installation and use of remote maintenance and diagnostic links.

https://t.me/learningnets

- Require that remote maintenance or diagnostic services be performed from a system that implements a level of security at least as high as that implemented on the system being serviced or remove the component to be serviced from the system and, prior to remote maintenance or diagnostic services, sanitize the component (for example, clearing of set points, embedded network addresses and embedded security validation information). After the service is performed and the component is returned to the facility, the organization should check or reinstall the authorized firmware code as specified by the configuration management plan and reset all authorized embedded configuration settings. Do this before reconnecting the component to the system to remove potentially malicious software that was added via "new" firmware.
- Require that remote maintenance sessions be protected by a strong authenticator tightly bound to the user.
- Require that maintenance personnel notify the system administrator when remote maintenance is planned (that is, date/time).
- Require that a designated organizational official with specific security/system knowledge approve the remote maintenance.
- Implement cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.
- Employ remote disconnect verification at the termination of remote maintenance and diagnostic sessions.

12.5 Electronic Communications

Often the focus of enterprise security is protecting stored information and server facilities, as well as client/server communication from the wide variety of threats on the landscape. It is important not to overlook security related to electronic communications that may not involve server or database access but that is between individuals. This section looks at four types of electronic communications that need to be protected.

Email

It is useful to have a basic grasp of the Internet mail architecture, as defined in RFC 5598, *Internet Mail Architecture*. At its most fundamental level, the Internet mail architecture consists of a user world, in the form of message user agents (MUAs), and a transfer world, in the form of the Message Handling System (MHS), which is composed of message transfer agents (MTAs). The MHS accepts a message from one user and delivers it to one or more other users, creating a virtual MUA-to-MUA exchange environment. This architecture involves three types of interoperability. One is directly between users: Messages must be formatted by the MUA on behalf of the

https://t.me/learningnets

message author so that the message are displayed to the message recipient by the destination MUA. There are also interoperability requirements between the MUA and the MHS—first when a message is posted from an MUA to the MHS and later when it is delivered from the MHS to the destination MUA. Interoperability is required among the MTA components along the transfer path through the MHS.

Figure 12.9 illustrates the key components of the Internet mail architecture.

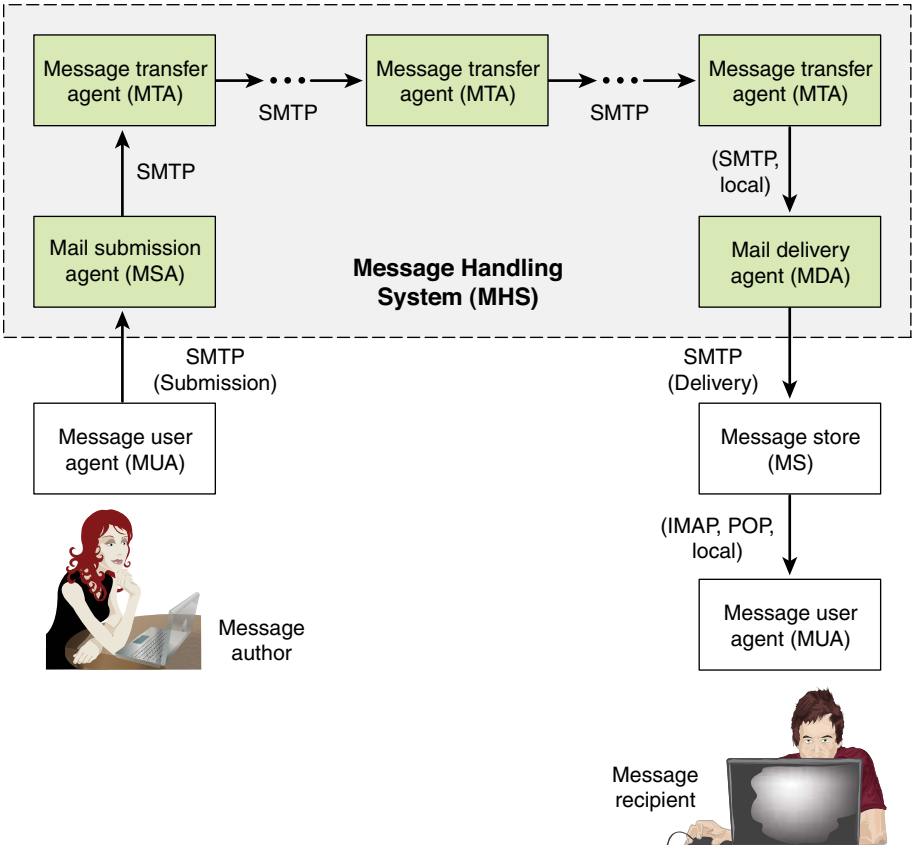


FIGURE 12.9 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture

The key components include the following:

- **Message user agent (MUA):** The MUA operates on behalf of user actors and user applications. It is their representative within the email service. Typically, this function is housed in the user's computer and is referred to as a

https://t.me/learningnets

client email program or a local network email server. The author MUA formats a message and performs initial submission into the MHS via a MSA. The recipient MUA processes received mail for storage and/or display to the recipient user.

- **Mail submission agent (MSA):** The MSA accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards. This function is either located together with the MUA or as a separate functional model. In the latter case, Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.
- **Message transfer agent (MTA):** The MTA relays mail for one application-level hop. It is like a packet switch or an IP router in that its job is to make routing assessments and to move the message closer to the recipients. Relaying is performed by a sequence of MTAs until the message reaches a destination MDA. An MTA also adds trace information to the message header. SMTP is used between MTAs and between an MTA and an MSA or MDA.
- **Mail delivery agent (MDA):** The MDA is responsible for transferring the message from the MHS to the MS, using SMTP.
- **Message store (MS):** The MUA employs a long-term MS, located on a remote server or on the same machine as the MUA. Typically, an MS retrieves messages from a remote MS using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).

Trustworthy Email Standards

For both organizations and individuals, email is pervasive and vulnerable to a wide range of security threats. In general terms, email security threats are classified as follows:

- **Authenticity-related threats:** Can result in unauthorized access to an enterprise's email system. Another threat in this category is deception, in which case the purported author isn't the actual author.
- **Integrity-related threats:** Can result in unauthorized modification of email content.
- **Confidentiality-related threats:** Can result in unauthorized disclosure of sensitive information.
- **Availability-related threats:** Can prevent end users from being able to send or receive email.

https://t.me/learningnets

To assist in addressing these threat categories, the National Institute of Standards and Technology (NIST) issued SP 800-177, *Trustworthy Email*, which provides recommendations and guidelines for enhancing trust in email. The document is both a survey of available standardized protocols and a set of recommendations for using these protocols to counter security threats to email usage. The following protocols and standards are described in and recommended by SP 800-177:

- **STARTTLS:** This SMTP security extension enables an SMTP client and server to negotiate the use of Transport Layer Security (TLS) to provide private, authenticated communication across the Internet.
- **S/MIME:** S/MIME provides authentication, integrity, non-repudiation (via digital signatures) and confidentiality (via encryption) of the message body carried in SMTP messages.
- **DNS-based Authentication of Named Entities (DANE):** DANE is designed to overcome problems in a certification authority (CA) system by providing an alternative channel for authenticating public keys based on DNSSEC (DNS Security Extensions), with the result that the same trust relationships used to certify IP addresses are used to certify servers operating on those addresses.
- **Sender Policy Framework (SPF):** SPF enables a domain owner to specify the IP addresses of MTAs that are authorized to send mail on its behalf. SPF uses DNS to allow domain owners to create records that associate the domain name with a specific IP address range of authorized MTAs. It is a simple matter for receivers to check the SPF TXT record in DNS to confirm that the purported sender of a message is permitted to use that source address and reject mail that does not come from an authorized IP address.
- **DomainKeys Identified Mail (DKIM):** DKIM enables an email actor (author or operator) to affix a domain name to the message reliably, using cryptographic techniques, so that filtering engines develop an accurate reputation for the domain. The MTA is able to sign selected headers and the body of a message. This validates the source domain of the mail and provides message body integrity.
- **Domain-based Message Authentication, Reporting and Conformance (DMARC):** DMARC publishes a requirement for the author domain name to be authenticated by DKIM and/or SPF, for that domain's owner to request recipient handling of non-authenticated mail using that domain, and a reporting mechanism from recipients back to domain owners. DMARC lets senders know the proportionate effectiveness of their SPF and DKIM policies and signals to receivers what action should be taken in various individual and bulk attack scenarios.

https://t.me/learningnets

An examination of these standards is beyond the scope of this book. For a detailed discussion, see Stallings's article "Comprehensive Internet Email Security" [STAL16]. A security manager must be aware of these standards and determine whether they should be required for email software products and services.

Another useful NIST document is SP 800-45, *Guidelines on Electronic Mail Security*, which complements SP 800-177. SP 800-45 recommends security practices for designing, implementing, and operating email systems on public and private networks. SP 800-177 focuses on the required Internet protocols and the use of digital signatures and encryption.

Acceptable Use Policy for Email

Many organizations provide email accounts for their employees that enable email to be sent and received within the organization as well as via the Internet. For such employees, it is recommended that an acceptable use policy be defined and agreed to by the employees. (See Section 4.3 for a general discussion of acceptable use policies.) As an example, an email acceptable use policy may include the following:

- **Acceptable behavior:** Use of email by employees is permitted and encouraged where such use supports the goals and objectives of the business.
- **Unacceptable behavior:** The following behavior by an employee is considered unacceptable:
  - Use of company communications systems to set up personal businesses or send chain letters
  - Forwarding of company confidential messages to external locations
  - Distributing, disseminating, or storing images, text, or materials that are considered indecent, pornographic, obscene, or illegal
  - Distributing, disseminating, or storing images, text, or materials that are considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or considered harassment
  - Accessing copyrighted information in a way that violates the copyright
  - Breaking into the company's or another organization's system or unauthorized use of a password/mailbox
  - Broadcasting unsolicited personal views on social, political, religious, or other non-business-related matters
  - Transmitting unsolicited commercial or advertising material

https://t.me/learningnets

- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

- **Monitoring:** The organization accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact on employee productivity and the reputation of the business. In addition, all of the company's email resources are provided for business purposes. Therefore, the company maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check up on the use and content of emails. Such monitoring is for legitimate purposes only and is undertaken in accordance with a procedure agreed with employees.
- **Sanctions:** Where it is believed that an employee failed to comply with this policy, he or she faces the company's disciplinary procedure. An employee who has breached the policy faces a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied depends on factors such as the seriousness of the breach and the employee's disciplinary record.
- **Agreement:** All company employees, contractors, or temporary staff who are granted the right to use the company's email services are required to sign this agreement, confirming their understanding and acceptance of the policy.

Security Policy for Email

In addition to an acceptable use policy, an organization needs a security policy for email that specifies how email is to be handled, transmitted, and stored. ISO 27002, *Code of Practice for Information Security Controls*, includes the following considerations for protecting email:

- Protecting messages from unauthorized access, modification, or denial of service commensurate with the classification scheme adopted by the organization
- Ensuring correct addressing and transportation of the message
- Ensuring reliability and availability of the service
- Considering legal factors, such as requirements for electronic signatures
- Obtaining approval prior to using external public services such as instant messaging, social networking, or file sharing
- Specifying stronger levels of authentication to control access from publicly accessible networks

https://t.me/learningnets

Instant Messaging

IM is a communications service in which short messages appear in pop-up screens as soon as they are received, thereby commanding the recipient's immediate attention. IM uses a shared software client between or among two or more people using personal computers, smartphones, or other devices. The communication is done over a network, often the Internet, and can include advanced modes with live voice or video. File transfers are also sometimes allowed but are limited in size. Most IM services offer presence information that indicates whether a user is online and available to send and receive messages. These services also provide *buddy lists*, which are groups of people the user has selected for frequent access, as well as group-based chat services. Enterprise IM provides real-time message passing within private and public networks.

Although included in the online chat category of technologies, IM differs in that the communicating parties are selected from the buddy list, and users are typically alerted when someone on their list is online. In contrast, online chat allows communication in a multiuser environment among users who are usually anonymous.

IM also differs from text messaging. The primary difference is that text messaging is a cellular phone service that is typically limited to 160 characters, whereas instant messaging is usually a computer session with a longer message size. After a text message is transmitted, the session is essentially ended even though the recipient can respond and keep the back-and-forth going all day. When an instant messaging session is started, it remains connected until the session is ended by one of the parties.

Acceptable Use Policy for IM



Instant Messaging Usage & Security Policy https://www.infotech.com/research/instant-messaging-usage-and-security-policy

A template for an instant messaging acceptable use policy developed by InfoTech includes the following rules that comprise the policy:

1. **Supported IM Solution:** [Company Name] has selected [name IM solution] as its sole provider of corporate IM services. Non-sanctioned IM services could affect network security, so the corporate firewall has been configured to block them. Free IM services commonly used within the consumer market are NOT approved or supported by the IT department.
2. **Acceptable Use:** IM services are to be used for business communications and for the purpose of fulfilling job duties, in accordance with corporate goals and objectives. Use of IM communications in this manner between [Company Name] employees and project teams is permitted and encouraged. It is expected that all employees will communicate professionally with colleagues, keeping in mind that foul language and slang terms are not allowed. [Note: If IT allows external IM communications with business partners or clients, these can be referred to here. However, this should only be done with added security features provided by IM security vendors.]

https://t.me/learningnets

3. **Confidentiality:** The transmission of sensitive corporate information through IM for business purposes is not permitted. Truly sensitive communications should be conducted through encrypted email or in-person meetings. Employees are prohibited from sending client lists, personal information, credit card information, trade secrets, and other proprietary information through the corporate IM service. In addition, it is prohibited to discuss legal advice or questions through IM with corporate lawyers, as this can violate the attorney-client privilege.
4. **File Sharing:** Though many IM services support the transmission of files, this feature has been blocked for IM at [Company Name]. [Note: Although Info-Tech recommends the banning of file sharing altogether, if advanced network-based security controls are in place, this section can be modified to include that file sharing is permitted and that all files will be automatically scanned for viruses and monitored by IT.]
5. **Personal Use:** Limited personal use of corporate IM services to communicate internally with colleagues at [Company Name] regarding non-work-related matters is permitted during designated work breaks and lunch hours only. Even during allotted personal IM usage periods, employees may not use the service for unsolicited mass mailings, non-[Company Name] commercial activity, operation of a privately owned business, solicitation of funds, dissemination of political causes, or promotion of religious/personal beliefs to others.
6. **Compliance:** IM use at [Company Name] will comply with, all [Company Name] policies, all [Company Name] contracts and all applicable laws.
7. **Privacy:** IM conversations and messages created on the corporate IM service and transmitted through corporate systems will be considered the property of [Company Name]. [Company Name] reserves the right to monitor, inspect, copy, review, store, and audit IM usage and messages generated by or for the enterprise. [Company Name] is also obligated to disclose IM messages and conversations when ordered to do so by auditors, courts, and law enforcement, with or without the employee's consent. Given these factors, employees do not have a reasonable expectation of privacy when using corporate IM services.

Security Policy for IM

IM is often poorly supervised, even though it introduces various risks to enterprise networks. Threats include IM-borne viruses, worms, spam over IM (SPIM), malware and phishing attacks, accidental or deliberate data leakage, inappropriate use, and regulatory noncompliance. A primary type of IM attack is to trick potential victims into installing a malicious program. IM-based attacks need some form of user interaction in order to launch, and attackers make use of social engineering to entice them

https://t.me/learningnets

to break security procedures or ignore common sense. These attacks usually exploit people's innate curiosity or natural desire to help. They also try to appeal to vanity or authority and other triggers, such as greed, fear, anger, or moral duty.

Thus, if an enterprise is going to enable employees to use IM, a corporate IM security policy is essential, and it needs to be backed up by user awareness training and an acceptable use policy.

Two basic approaches enable an enterprise to maintain security over IM. Both approaches limit employees to the use of the enterprise-mandated IM facility and further limit the group of employees that can use IM. One approach is to host an enterprise IM server in-house. This enables the enterprise to enforce its IM policies through traffic analysis and reporting, message keyword searches, and message archiving. The enterprise can also implement end-to-end encryption and user authentication, as well as configure content and URL filters and allow the controlled use of many collaboration features, such as integrated live voice, video, and data.

The enterprise may also opt for a cloud service, which means there is no need to install additional hardware or software. All IM messages sent to or from the enterprise network are routed through the cloud service, where they are scanned for viruses, worms, and malicious URLs. Messages are also matched against enterprise content control and acceptable IM use policies: Messages that are malicious or suspicious or that violate policies are automatically blocked. Also, all messages are logged and can be sent to the enterprise's existing archiving solution to satisfy legal discovery requirements and other relevant regulations. This type of service makes enterprise-grade control of IM accessible to organizations of all sizes.

Voice over IP (VoIP) Networks

VoIP has become increasingly prevalent in organizations of all sizes. In essence, VoIP involves the transmission of speech across IP-based network. VoIP works by encoding voice information into a digital format, which is carried across IP networks in discrete packets. VoIP has two main advantages over traditional telephony:

- A VoIP system is usually cheaper to operate than an equivalent telephone system with a PBX and conventional telephone network service. There are several reasons for this. Whereas traditional telephone networks allocate dedicated circuits for voice communications using circuit switching, VoIP uses packet switching, allowing the sharing of transmission capacity. Further, packetized voice transmission fits well in the framework of the TCP/IP protocol suite, enabling the use of application- and transport-level protocols to support communications.
- VoIP readily integrates with other services, such as combining web access with telephone features through a single PC or terminal.

https://t.me/learningnets

VoIP Signaling

Before voice is transferred using VoIP, a call must be placed. In a traditional phone network, the caller enters the digits of the called number. The telephone number is processed by the provider's signaling system to ring the called number. With VoIP, the calling user (program or individual) supplies the phone number of a URI (universal resource indicator, a form of URL), which then triggers a set of protocol interactions and results in the placement of the call.

The heart of the call placement process for VoIP is the Session Initiation Protocol (SIP), defined in RFC 3261, which is an application-level control protocol for setting up, modifying, and terminating real-time sessions between participants over an IP data network. SIP supports not only VoIP but also many multimedia applications. Associated with SIP is Session Description Protocol (SDP), defined in RFC 4566. SIP is used to invite one or more participants to a session, and the SDP-encoded body of a SIP message contains information about what media encodings (for example, voice, video) the parties can and will use. Once this information is exchanged and acknowledged, all participants are aware of the participants' IP addresses, available transmission capacity, and media type. Then data transmission begins, using an appropriate transport protocol. Typically, Real-Time Transport Protocol (RTP) is used. Throughout the session, participants can make changes to session parameters, such as new media types or new parties to the session, using SIP messages.

An alternative to the use of SIP is ITU-T H.323. The H.323 protocol has been available for several years, and carriers made a significant investment to build out many large, H.323-based networks. SIP is growing in popularity due to its ability to easily combine voice and Internet-based services. SIP interoperability and coexistence with H.323 is very important to maximize the return on current investments and to support new deployments that might use SIP as an alternative packet telephony signaling protocol.

VoIP Processing

In a VoIP system, when a called party responds, a logical connection is established between the two parties (or more parties, for a conference call), and voice data can be exchanged in both directions. Figure 12.10 illustrates the basic flow of voice data in one direction in a VoIP system. On the sending side, the analog voice signal is first converted into a digital bit stream and then segmented into packets. The packetization is performed, typically, by RTP. This protocol includes mechanisms for labeling the packets so that they can be reassembled in the proper order at the receiving end, plus a buffering function to smooth out reception and deliver the voice data in a continuous flow. The RTP packets are then transmitted across the Internet or a private intranet using User Datagram Protocol (UDP) and IP.

https://t.me/learningnets

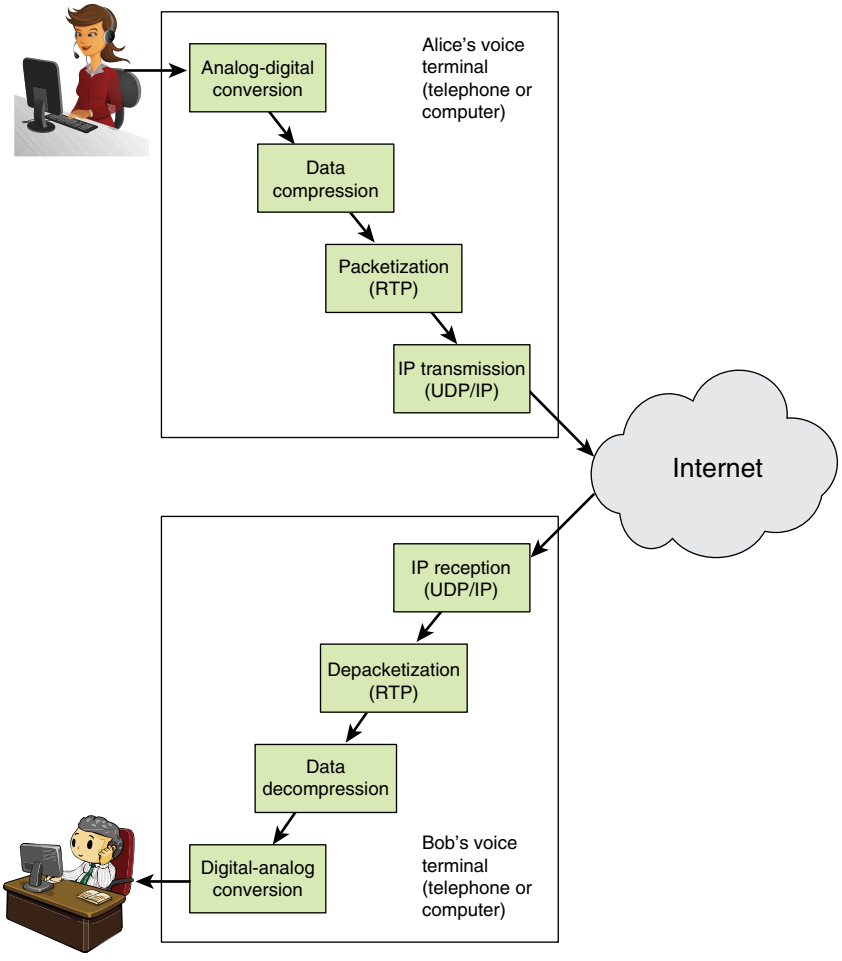


FIGURE 12.10 VoIP Processing

At the receiving end, the process is reversed. The packet payloads are reassembled by RTP and put into the proper order. The data are then decompressed, and the digitized voice is processed by a digital-to-analog converter to produce analog signals for the receiver's telephone or headset speaker.

VoIP Context

Ultimately, VoIP using IP-based networks may replace the public circuit-switched networks in use today. But for the foreseeable future, VoIP must coexist with the existing telephony infrastructure. Figure 12.11 shows some of the key elements involved in the coexistence of these older and newer technologies.

https://t.me/learningnets

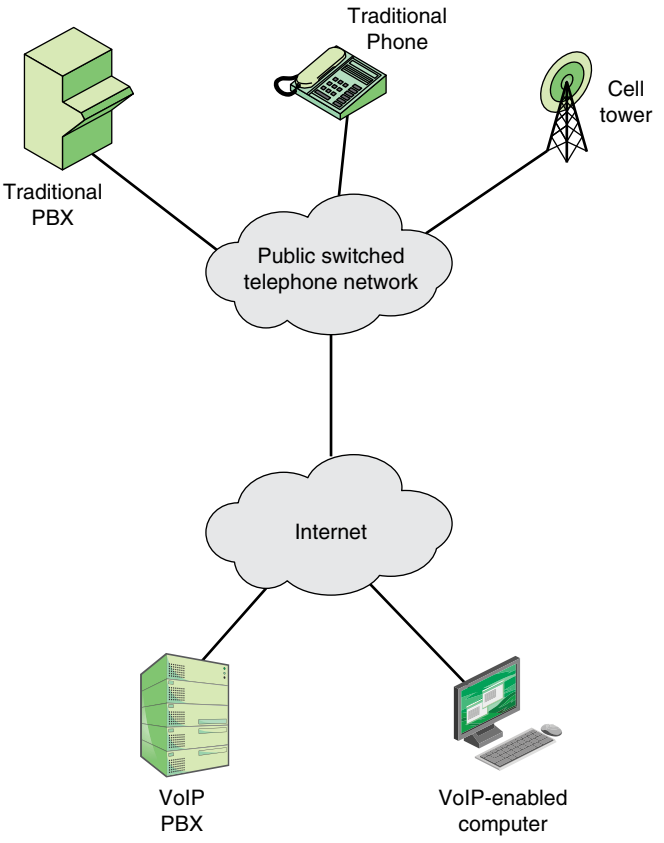


FIGURE 12.11 VoIP Context

The deployment of the VoIP infrastructure is accompanied by a variety of end-user products, including the following:

- **Traditional telephone handset:** These corded or cordless units function much like traditional telephones but are VoIP capable. They typically have many additional features, making use of a screen, and providing capabilities similar to those of smartphones.
- **Conferencing units:** These provide the same basic service as conventional conference calling phone systems and also allow users to coordinate other data communications services, such as text, graphics, video, and whiteboarding.
- **Mobile units:** Smartphones and other cellphones with VoIP capability can tie directly into a VoIP network without needing to go through any kind of gateway system.

https://t.me/learningnets

- **Softphone:** The term *softphone* refers to software operating on a PC that implements VoIP. Typically, the PC is configured with a headset or with a telephone that makes use of a USB connection to the PC.

A wide variety of infrastructure equipment has been developed to support VoIP. There are two noteworthy types:

- **IP PBX:** The IP PBX is designed to support digital and analog phones and connect to IP-based networks using VoIP, as well as provide a connection to the public switched telephone network using traditional technology, if needed.
- **Media gateway:** The media gateway connects different physical networks in order to provide end-to-end connectivity. An important type of media gateway connects a VoIP network to a circuit-switched telephone network, providing the necessary conversion and signaling.

The VoIP environment continues to evolve, and a large number of products are being developed for providers, businesses, and residential/personal users.

VoIP Threats

As VoIP becomes mainstream, a number of security issues must be understood and addressed. Key areas of concern are as follows:

- VoIP traffic travels through the Internet. It is possible that a hacker could use a packet sniffer to listen to unencrypted VoIP traffic. The solution lies in setting up a VPN between the endpoints, but doing so also introduces additional complications.
- Many older firewalls may not recognize VoIP packets. In addition, some intrusion detection systems may try to inspect voice packets, thereby introducing delay and jitter. Bypassing the traffic inspection rules in the firewall may create additional vulnerability.
- Many older VoIP phones may require security patches for their software. Such patches are seldom applied as many administrators are not even aware that phone software needs to be patched. Some VoIP phones are set up to apply patches directly without even asking for authentication. Such phones can be very vulnerable to hackers.
- Phones also inherit the security flaws of the operating systems they use.
- Systems used out of the box may have default passwords and open ports that need to be managed and secured. In many cases, this is ignored.
- DoS attacks can be launched against a VoIP phone system, just as they can be launched against other computer applications.

https://t.me/learningnets

The following are some specific threats to the use of VoIP:

- **Spam over Internet telephone (SPIT):** Unsolicited bulk messages may be broadcast over VoIP to phones connected to the Internet. Although marketers already use voicemail for commercial messages, IP telephony makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately.
- **Eavesdropping:** Interception of control packets enables an adversary to listen in on an unsecured VoIP call.
- **Theft of service:** This type of attack involves capturing access codes, allowing the adversary to get into the VoIP provider network and then use the facility.
- **Man-in-the middle attack:** This type of attack involves an adversary inserting as a relay point between two ends of a VoIP call. In addition to eavesdropping, the adversary could divert a call to a third party or generate simulated voice content to create misleading impressions or cause operational errors.

VoIP Security Measures

A number of security measures can be taken to protect VoIP traffic, including the following:

- **Encryption:** It is a good practice to encrypt all voice connections.
- **VPNs:** VPNs create segregated broadcast domains within the IP network infrastructure. By creating VPNs for voice, organizations provide an additional layer of protection that can potentially insulate voice communications from DoS attacks and other risks.
- **Port administration:** SIP applications tend to open multiple ports on network devices, creating additional exposure to hackers. Therefore, IT staff need to implement firewalls and other security administration tools that discover and close unnecessarily opened ports—and rigorously authenticate devices attempting to use those ports.
- **Real-time antivirus scanner:** An organization should scan the VoIP server continuously.
- **Application-layer firewall:** This protects assets associated with the VoIP server, such as a database devoted to logging calls or even recording the calls.
- **Device authentication:** Any user device that attempts to use the VoIP service should be authenticated.
- **User authentication:** Individual users should be authenticated to limit specific users or groups of users to specific VoIP services.

https://t.me/learningnets

Telephony and Conferencing

The security objective with respect to telephony and conferencing is to prevent and detect unauthorized use or misuse of telephony and conferencing facilities. This is achieved with a combination of physical and logical controls. The SGP recommends that there should be policies that cover the following:

- Use of the organization's telephones
- Moves and changes of telephone users
- Registration and authentication of users with access to voicemail
- Protection of voicemail systems against unauthorized access (for example, by use of password protection)
- The use and setup of web-based conferencing facilities (including teleconferencing, videoconferencing, and online web-based collaboration)

12.6 Networks and Communications Best Practices

The SGP breaks down best practices in the networks and communication category into 2 areas and 10 topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Network management:** The objectives of this area are to (1) design physical, wireless, and voice networks to be reliable and resilient; prevent unauthorized access; encrypt connections; and detect suspicious traffic and (2) configure network devices (including routers, firewalls, and wireless access points) to function as required and to prevent unauthorized or incorrect updates.
  - **Network device configuration:** Lists the key practices to ensure that network devices (including routers, switches, and firewalls) are configured to function as required and to prevent unauthorized or incorrect updates.
  - **Physical network management:** Addresses issues related to the physical protection of network devices and communications links.
  - **Wireless access:** Provides a policy checklist for managing wireless access.
  - **External network connections:** Provides a policy checklist for managing and protecting external network connections.

https://t.me/learningnets

- **Firewalls:** Details the types of firewalls to be used and provides guidelines for firewall security policy.
- **Remote maintenance:** Lists measures to protect remote maintenance facilities from misuse.

- **Electronic communications:** The objectives of this area are to protect electronic communication systems by setting policy for their use; configuring security settings; and hardening the supporting technical infrastructure. Four topics are covered: email, instant messaging, VoIP, and telephone/conferencing. For each of these topics, the SGP provides checklists of policies and procedures to secure against misuse.

12.7 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms.

accounting management
application-level gateway
circuit-level gateway
configuration management
DMZ network
Email
Fault
fault management
firewall
instant messaging
IP Security (IPsec)
Message Handling System (MHS)
message store (MS)
message submission agent (MSA)
message transfer agent (MTA)
message user agent (MUA)
network management
network management system
packet filtering firewall
performance management
security management
stateful inspection firewall
virtual private network (VPN)
voice over IP (VoIP)

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. According to ISO 7498-4, what are the key functions of network management?
2. What are some of the key tasks performed by a network management entity?
3. How is a distributed network management system organized?
4. Explain the network management architecture defined by Cisco.

https://t.me/learningnets

5. Name all the techniques that firewalls use to control access to a site and enforce the site's security policy.
6. What are some common types of firewalls?
7. What are some of the weaknesses of packet filters?
8. What are some of the important characteristics of automated network device configuration management tools?
9. According to TIA-942, which functional areas are included in a data center?
10. What are some of the key risks associated with wireless access?
11. According to SP 800-41, how are firewall planning and implementation phases defined?
12. In general, how can you classify email security threats?
13. According to ISO 27002, how can an organization protect email?
14. Describe two types of infrastructure equipment that support VoIP.
15. What are some of the principal threats to VoIP usage?
16. How does the Standards Customer Council define the key components of a cloud service agreement (CSA)?

12.8 References

BALA15: Balasubramanian, V., *Conquering the Operational Challenges of Network Change & Configuration Management Through Automation.* Zoho Corp. white paper, 2015. https://www.manageengine.com/network-configuration-manager/network-configuration-management-overview.html

BANK14: Banks, E., "Automating Network Device Configuration." *Network World*, July 2014.

BELL94: Bellovin, S., and Cheswick, W. "Network Firewalls." *IEEE Communications Magazine*, September 1994.

BEUC09: Buecker, A., Andreas, P., & Paisley, S., *Understanding IT Perimeter Security*. IBM red paper REDP-4397-00, November 2009.

https://t.me/learningnets

CISC07: Cisco Systems, *Cisco Advanced Services Network Management Systems Architectural Leading Practice.* White Paper C07-400447-00, September 2007. https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb4c.pdf

DHS11: U.S. Department of Homeland Security. *Catalog of Control Systems Security: Recommendations for Standards Developers.* Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, April 2011.

KENN03: Kennedy, S., "Best Practices for Wireless Network Security." *ComputerWorld*, November 23, 2003.

STAL16: Stallings, W., "Comprehensive Internet Email Security." *Internet Protocol Journal*, November 2016. Available at http://williamstallings.com/Papers/

https://t.me/learningnets

Chapter 13

Supply Chain Management and Cloud Security

We cannot enter into alliance with neighboring princes until we are acquainted with their designs.

—*The Art of War*, Sun Tzu

Learning Objectives

After studying this chapter, you should be able to:

- Understand the essential concepts of supply chain management.
- Make a presentation concerning the application of risk management and risk assessment policies to supply chains.
- Present an overview of cloud computing concepts.
- List and define the principal cloud services.
- List and define the cloud deployment models.
- Discuss key management concerns related to cloud service security.
- Present an overview of supply chain best practices.
- Discuss the differences between document management and records management.
- Present an overview of the considerations involved in protecting sensitive physical information.
- Present an overview of information management best practices.

This chapter is concerned with security services related to the use of external providers/vendors of products and services. It begins with an introduction to the concept of supply chain and supply chain management issues. Next, it examines the application of risk management and risk assessment policies and procedures to the security concerns related to supply chain management.

https://t.me/learningnets

The remainder of the chapter looks at significant type of external provision, namely cloud computing services, and deals with the issues peculiar to this topic. Section 13.3 introduces basic concepts of cloud computing, and Section 13.4 discusses cloud security from the point of view of the cloud service customer.

13.1 Supply Chain Management Concepts

As enterprises pursue outsourcing strategies and their supply and delivery systems become increasingly global, the visualizing, tracking, and management of supply chains becomes increasingly complex. A significant reliance on supply chains also introduces increased risk into the organization. This section introduces the basic concepts of the supply chain and supply chain management and sets the stage for an examination of security aspects of supply chain management in Section 13.2.

The Supply Chain

Traditionally, a *supply chain* was defined as the network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product, from the delivery of source materials from the supplier to the manufacturer, through to its eventual delivery to the end user. In this traditional use, the term applies to the entire chain of production and use of physical products. The chain can link a number of entities, beginning with raw materials suppliers, through manufacturers, wholesalers, retailers, and consumers.

More recently the term *supply chain* has been used in connection with **information and communications technology (ICT)**. National Institute of Standards and Technology (NIST) SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, defines the term *ICT supply chain* as follows:

> Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer. *Note*: An ICT supply chain can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the design and development, manufacturing, processing, handling, and delivery of the products, or service providers involved in the operation, management, and delivery of the services.

information and communications technology (ICT)
Refers to the collection of devices, networking components, applications, and systems that together allow people and organizations to interact in the digital world. ICT is sometimes used synonymously with IT; however, ICT represents a broader, more comprehensive list of all components related to computer and digital technologies than IT.

https://t.me/learningnets

Figure 13.1 is a simplified view of the flows in an ICT supply chain.

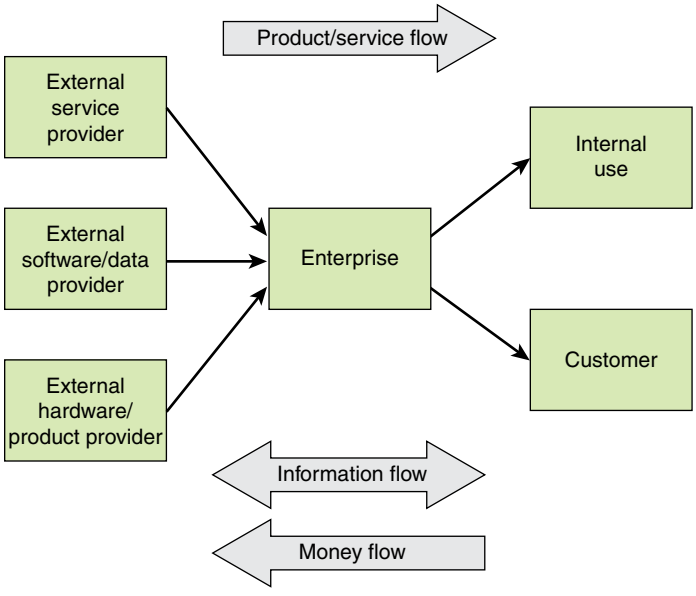


FIGURE 13.1 Supply Chain Flows

An enterprise procures the following from external sources:

- **Services:** Examples include cloud computing services, data center services, network services, and external auditing services.
- **Software/data:** Examples include operating system and application software and databases of information, such as threat information.
- **Hardware/products:** Examples include computer and networking equipment.

The procured items are often for internal use but can be packaged, integrated, or otherwise prepared for sale to external customers.

Figure 13.1 indicates three types of flows associated with a supply chain:

- **Product/service flow:** A key requirement is a smooth flow of an item from the provider to the enterprise and then on to the internal user or external customer. The quicker the flow, the better it is for the enterprise, as it minimizes the cash cycle.
- **Information flow:** Information flow comprises the request for quotation, purchase order, monthly schedules, engineering change requests, quality complaints, and reports on supplier performance from the customer side to

https://t.me/learningnets

the supplier. From the producer's side to the consumer's side, the information flow consists of the presentation of the company, offer, confirmation of purchase order, reports on action taken on deviation, dispatch details, report on inventory, invoices, and so on.

- **Money flow:** On the basis of the invoice raised by the producer, the clients examine the order for correctness. If the claims are correct, money flows from the clients to the respective producer. Flow of money is also observed from the producer side to the clients in the form of debit notes.

Supply Chain Management

Supply chain management (SCM) is the active management of supply chain activities to maximize customer value and achieve a sustainable competitive advantage. It represents a planned initiative by the enterprises to develop and run supply chains in the most effective and efficient ways possible. Supply chain activities cover everything from product development, sourcing, production, and logistics to the information systems needed to coordinate these activities.

Figure 13.2 illustrates a typical sequence of elements involved in supply chain management.

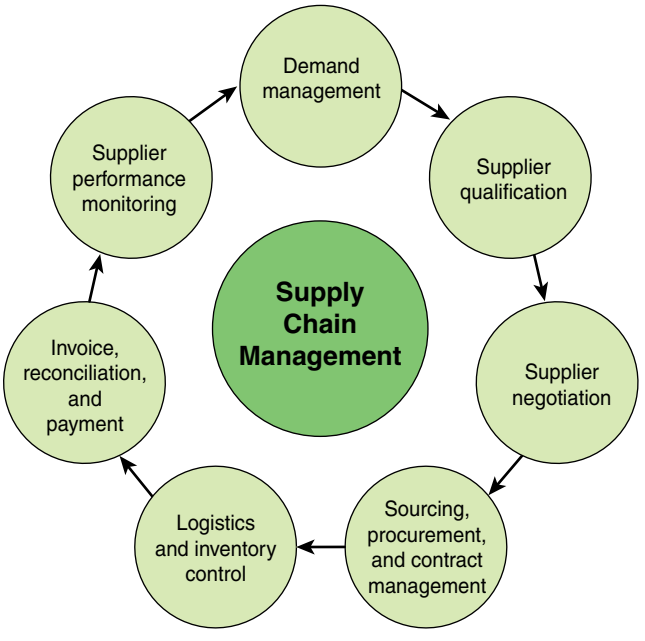


FIGURE 13.2 Supply Chain Management

https://t.me/learningnets

The elements of supply chain management include the following:

- **Demand management:** This function recognizes all demands for goods and services to support the marketplace. It involves prioritizing demand when supply is lacking. Proper demand management facilitates the planning and use of resources for profitable business results.
- **Supplier qualification:** This function provides an appropriate level of confidence that suppliers, vendors, and contractors are able to supply consistent quality of materials, components, and services in compliance with customer and regulatory requirements. An integrated supplier qualification process should also identify and mitigate the associated risks of materials, components, and services.
- **Supplier negotiation:** In this process of formal communication, two or more people come together to seek mutual agreement on an issue or issues. Negotiation is particularly appropriate when issues besides price are important for the buyer or when competitive bidding does not satisfy the buyer's requirements on those issues.
- **Sourcing, procurement, and contract management:** *Sourcing* refers to the selection of a supplier or suppliers. *Procurement* is the formal process of purchasing goods or services. *Contract management* is a strategic management discipline employed by both buyers and sellers whose objectives are to manage customer and supplier expectations and relationships, control risk and cost, and contribute to organizational profitability/success. For successful service contract administration, the buyer needs to have a realistic degree of control over the supplier's performance. Crucial to success in this area is the timely availability of accurate data, including the contractor's plan of performance and the contractor's actual progress.
- **Logistics and inventory control:** In this context, logistics refers to the process of strategically managing the procurement, movement, and storage of materials, parts, and finished inventory (and the related information flows) through the organization and its marketing channels. Inventory control is the tracking and accounting of procured items.
- **Invoice, reconciliation, and payment:** This is the process of paying for goods and services.
- **Supplier performance monitoring:** This function includes the methods and techniques for collecting information to be used to measure, rate, or rank supplier performance on a continuous basis. *Performance* refers to the ability of the supplier to meet stated contractual commitments and enterprise objectives.

https://t.me/learningnets

13.2 Supply Chain Risk Management

Supply chain risk management (SCRM) is the coordinated efforts of an organization to help identify, monitor, detect, and mitigate threats to supply chain continuity and profitability. SCRM, in essence, applies the techniques of risk assessment, as discussed in Chapter 3, "Information Risk Assessment," to the supply chain. All the techniques discussed in that chapter are relevant to this discussion of SCRM.

NIST has published two useful documents related to SCRM. SP 800-161 describes the SCRM process, provides a detailed description of supply chain threats and vulnerabilities, and defines a set of security controls for SCRM. NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, focuses on best practices for SCRM. NIST also maintains a website devoted to SCRM that includes a number of industry papers on the subject.

Cyber Supply Chain Risk Management https://csrc.nist.gov/projects/supply-chain-risk-management/

Figure 13.3, from SP 800-161, illustrates the risk assessment process applied to the supply chain (compare Figure 13.1). Like any other form of risk assessment, SCRM risk assessment begins with an analysis of threats and vulnerabilities. As shown in Figure 13.3, threats come from either an adversarial source that intends deliberate harm or from a non-adversarial source, which is an unintentional threat. Vulnerabilities in the supply chain can be external to the organization or internal.

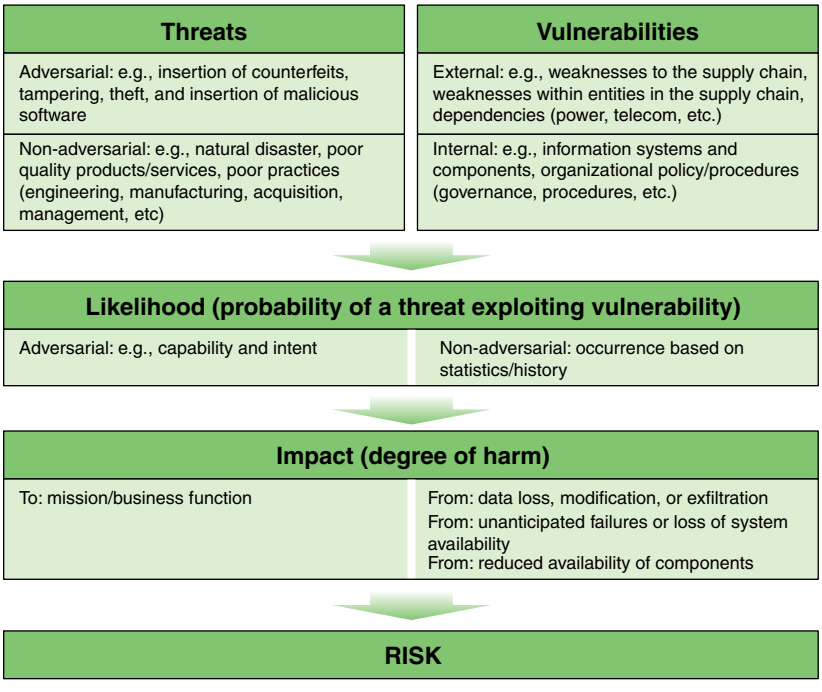


FIGURE 13.3 ICT Supply Chain Risk

https://t.me/learningnets

Once the threats and vulnerabilities are determined, it is possible to estimate the likelihood of a threat being able to exploit a vulnerability to produce harm. Risk assessment then involves determining the impact of the occurrence of various threat events.

Supply chain risk assessment is a specific example of the risk assessment done by an organization and is part of the risk management process depicted in Figures 3.2 and 3.3.

SP 800-161 makes use of a risk management model defined in SP 600-39, *Managing Information Security Risk*, shown in Figure 13.4. The model consists of three tiers:

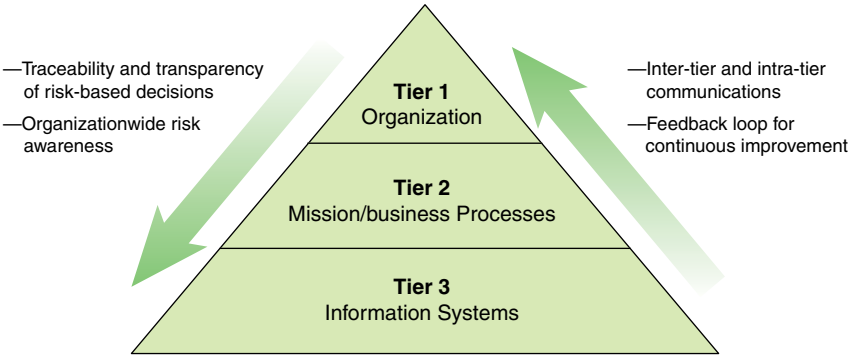


FIGURE 13.4 Multi-tiered Organizationwide Risk Management

- **Tier 1:** This tier is engaged in the development of the overall ICT SCRM strategy, determination of organization-level ICT SCRM risks, and setting of the organization-wide ICT SCRM policies to guide the organization's activities in establishing and maintaining organizationwide ICT SCRM capability.
- **Tier 2:** This tier is engaged in prioritizing the organization's mission and business functions, conducting mission/business-level risk assessment, implementing Tier 1 strategy and guidance to establish an overarching organizational capability to manage ICT supply chain risks, and guiding organizationwide ICT acquisitions and their corresponding system development life cycles (SDLCs).
- **Tier 3:** This tier is involved in specific ICT SCRM activities applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' SDLCs.

Richard Wilding's blog post "Classification of the Sources of Supply Chain Risk and Vulnerability" [WILD13] provides a useful perspective on categorizing supply chain risk areas. In general terms, supply chain risks may be either external or internal, as illustrated in Figure 13.5.

https://t.me/learningnets

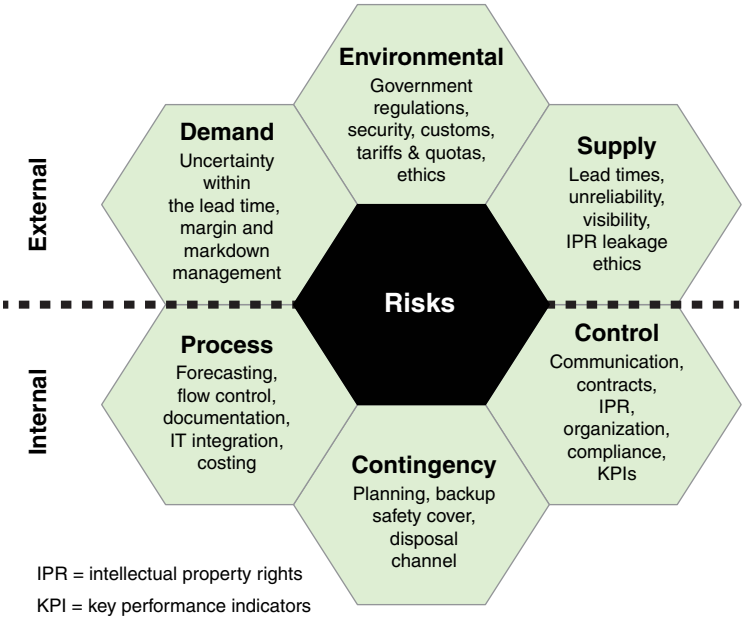


FIGURE 13.5 Supply Chain Risk Areas

The external risks are as follows:

- **Demand:** Refers to disturbances to the flow of product, information, or cash from within the supply chain between the organization and its market. For example, disruptions in the cash resource within the supply chain needed to pay the organization can have a major impact on the operating capability of organizations.
- **Supply:** The upstream equivalent of demand risk; it relates to potential or actual disturbances to the flow of product or information from within the supply chain between the organization and its suppliers. In a similar way to demand risk, the disruption of key resources coming into the organization can have a significant impact on the organization's ability to perform
- **Environmental:** The risk associated with external and, from the firm's perspective, uncontrollable events. The risks can impact the firm directly or through the firm's suppliers and customers. Environmental risk is broader than just natural events like earthquakes or storms. It also includes, for example, changes created by governing bodies such as changes in legislation or customs procedures, as well as changes in the competitive climate.

intellectual property rights (IPR)

Rights to the body of knowledge, ideas, or concepts produced by an entity that are claimed by that entity to be original and of copyright-type quality.

key performance indicators (KPIs)

Quantifiable measurements, agreed to beforehand, that reflect the critical success factors of an organization.

https://t.me/learningnets

The internal risks are as follows:

- **Processes:** The sequences of value-adding and managerial activities undertaken by the firm. Process risk relates to disruptions to key business processes that enable the organization to operate. Some processes are key to maintaining the organization's competitive advantage, while others can underpin the organization's activities.
- **Controls:** The rules, systems, and procedures that govern how an organization exerts control over processes and resources. In terms of the supply chain, controls may relate to order quantities, batch sizes, safety stock policies, and so on, plus the policies and procedures that govern asset and transportation management. Control risk is therefore the risk arising from the application or misapplication of these rules.
- **Contingency:** The existence of a prepared plan and the identification of resources that are mobilized in the event of a risk being identified. Contingency plans may encompass inventory, capacity, dual sourcing, distribution and logistics alternatives, and backup arrangements.

Supply Chain Threats

Table 13.1, from SP 800-161, provides examples of threat considerations and different methods that can be used to characterize ICT supply chain threats at different tiers. These considerations provide an organized way of approaching the threat analysis that is part of risk assessment.

TABLE 13.1 Supply Chain Threat Considerations

Tier	Threat Consideration	Methods
Tier 1	■ Organization's business and mission ■ Strategic supplier relationships ■ Geographic considerations related to the extent of the organization's ICT supply chain	■ Establish common starting points for identifying ICT supply chain threat. ■ Establish procedures for countering organizationwide threats such as insertion of counterfeits into critical systems and components.
Tier 2	■ Mission functions ■ Geographic locations ■ Types of suppliers (commercial off the shelf [COTS], external service providers, or custom, and so on) ■ Technologies used throughout the organization	■ Identify additional sources of threat information specific to organizational mission functions. ■ Identify potential threat sources based on the locations and suppliers identified through examining available agency ICT supply chain information.

https://t.me/learningnets

Tier	Threat Consideration	Methods
		■ Scope identified threat sources to the specific mission functions, using the agency the ICT supply chain information. ■ Establish mission-specific preparatory procedures for countering threats.
Tier 3	■ System development life cycle	■ Base the level of detail with which threats should be considered on the SDLC phase. ■ Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.

As indicated in Figure 13.3, threats are categorized as adversarial or non-adversarial. It is very useful for an organization to have a reliable list of the types of events in each category in order to ensure that all threats are considered in the threat analysis. Table 13.2, from SP 800-161, lists possible adversarial threat events, broken down into seven distinct areas. As shown, the task of threat analysis is formidable.

TABLE 13.2 Adversarial Supply Chain Threat Events

Event Category	Threat Event
Perform reconnaissance and gather information	■ Perform malware-directed internal reconnaissance
Craft or create attack tools	■ Craft phishing attacks ■ Craft attacks specifically based on the deployed IT environment ■ Create counterfeit/spoof websites ■ Craft counterfeit certificates ■ Create and operate false front organizations to inject malicious components into the supply chain
Deliver/insert/install malicious capabilities	■ Deliver known malware to internal organizational information systems (for example, virus via email) ■ Deliver modified malware to internal organizational information systems ■ Deliver targeted malware for control of internal systems and **exfiltration** of data ■ Deliver malware by providing removable media ■ Insert untargeted malware into downloadable software and/or into commercial IT products ■ Insert targeted malware into organizational information systems and information system components

exfiltration

A malware process that automates the sending of harvested victim data, such as login credentials and cardholder information, back to an attacker-controlled server.

https://t.me/learningnets

Event Category	Threat Event
	■ Insert specialized malware into organizational information systems based on system configurations ■ Insert counterfeit or tampered hardware into the supply chain ■ Insert tampered critical components into organizational systems ■ Insert malicious scanning devices (for example, wireless sniffers) inside facilities ■ Insert subverted individuals into organizations ■ Insert subverted individuals into privileged positions in organizations
Exploit and compromise	■ Insert subverted individuals into privileged positions in organizations (that is, systems that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections) ■ Exploit vulnerabilities in information systems timed with the organizational mission/business operations tempo ■ Exploit insecure or incomplete data deletion in a multitenant environment ■ Violate isolation in a multitenant environment ■ Compromise information systems or devices used externally and reintroduced into the enterprise ■ Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware)
Conduct an attack (that is, direct/coordinate attack tools or activities)	■ Conduct physical attacks on infrastructures supporting organizational facilities ■ Conduct internally based session hijacking ■ Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware
Achieve results (that is, cause adverse impacts, obtain information)	■ Cause unauthorized disclosure and/or unavailability by spilling sensitive information ■ Obtain information by externally located interception of wireless network traffic ■ Obtain unauthorized access ■ Obtain information by opportunistically stealing or scavenging information systems/component
Maintain a presence or set of capabilities	■ Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome ■ Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors

https://t.me/learningnets

In the category of non-adversarial threat events, SP 800-161 lists the following:

- An authorized user erroneously contaminates a device, an information system, or a network by placing on it or sending to it information of a classification/sensitivity that it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
- An authorized privileged user inadvertently exposes critical/sensitive information.
- A privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
- Processing performance is degraded due to resource depletion.
- Vulnerabilities are introduced into commonly used software products.
- Multiple disk errors may occur due to aging of a set of devices all acquired at the same time, from the same supplier.

Supply Chain Vulnerabilities

As with threats, SP 800-163 provides guidance on tier-based analysis of supply chain vulnerabilities. Table 13.3 provides a systematic way of working down from tier 1 through tier 3 to consider all vulnerabilities.

TABLE 13.3 Supply Chain Vulnerability Considerations

Tier	Vulnerability Consideration	Methods
Tier 1	■ Organization's mission/business ■ Supplier relationships (for example, system integrators, COTS, external services) ■ Geographic considerations related to the extent of the organization's ICT supply chain ■ Enterprise/security architecture ■ Criticality baseline	■ Examine agency ICT supply chain information, including that from supply chain maps, to identify especially vulnerable locations or organizations. ■ Analyze agency mission for susceptibility to potential supply chain vulnerabilities. ■ Examine system integrator and supplier relationships for susceptibility to potential supply chain vulnerabilities. ■ Review enterprise architecture and criticality baseline to identify areas of weakness requiring more robust ICT supply chain considerations.

https://t.me/learningnets

Tier	Vulnerability Consideration	Methods
Tier 2	■ Mission functions ■ Geographic locations ■ Types of suppliers (COTS, custom, and so on) ■ Technologies used	■ Refine analysis from tier 1 based on specific mission functions and applicable threat and supply chain information. ■ Consider using the National Vulnerability Database (NVD), including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), to characterize, categorize, and score vulnerabilities. ■ Consider using scoring guidance to prioritize vulnerabilities for remediation.
Tier 3	■ Individual technologies, solutions, and suppliers	■ Use CVEs where available to characterize and categorize vulnerabilities. ■ Identify weaknesses.

For example, in tier 1, a type of vulnerability is a deficiency or weakness in organizational governance structures or processes, such as a lack of an ICT SCRM plan. Ways to mitigate this vulnerability include providing guidance on how to consider dependencies on external organizations as vulnerabilities and seeking out alternative sources of new technology, including building in-house.

An example of a vulnerability at tier 2 is no budget being allocated for the implementation of a technical screening for acceptance testing of ICT components entering the SDLC as replacement parts. The obvious remedy is to determine a reasonable budget allocation.

An example of a vulnerability at tier 3 is a discrepancy in system functions not meeting requirements, resulting in substantial impact to performance. The mitigation approach is to initiate the necessary engineering change.

Supply Chain Security Controls

SP 800-161 provides a comprehensive list of security controls for SCRM. These controls are organized into the following families:

- Access control
- Awareness and training
- Audit and accountability
- Security assessment and authorization
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance

https://t.me/learningnets

- Media protection
- Physical and environmental protection
- Planning
- Program management
- Personnel security
- Provenance
- Risk assessment
- System and services acquisition
- System and communications protection
- System and information security

All these control families, with the exception of the provenance family, are adapted for the specific needs of SCRM from the security controls defined in SP 800-53.

Security control AC-3 (access enforcement) provides an example of the adaptation of a security control to SCRM security needs. In SP 800-53, the description of this security control begins as follows:

- **Control:** The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- **Supplemental Guidance:** Access control policies (for instance, identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (for example, access control lists, access control matrices, cryptography) control access between active entities or subjects (for example, users or processes acting on behalf of users) and passive entities or objects (for instance, devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems host many applications and services in support of organizational missions and business operations, access enforcement mechanisms are also employed at the application and service level to provide increased information security.
- **Control Enhancements:**

  (8) REVOCATION OF ACCESS AUTHORIZATIONS

  The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].
- **Supplemental Guidance:** Revocation of access rules differ based on the types of access revoked. For example, if a subject (that is, user or process) is removed from a group, access may not be revoked until the next time the object (for example, file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels can take effect immediately. Organizations can provide

https://t.me/learningnets

alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

The information system does not release information outside of the established system boundary unless:

- The receiving (Assignment: organization-defined information system or system component) provides (Assignment: organization-defined security safeguards); and
- (Assignment: organization-defined security safeguards) are used to validate the appropriateness of the information designated for release.

There are a total of 10 security enhancements for this control; we show only numbers 8 and 9 in this example.

The control section prescribes specific security-related activities or actions to be carried out by organizations or by information systems. The supplemental guidance section provides nonprescriptive additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate. The security control enhancements section provides statements of security capability to add functionality/specificity to a control and/or increase the strength of a control. In both cases, control enhancements are used in information systems and environments of operation requiring greater protection than provided by the base control due to the potential adverse organizational impacts or when organizations seek additions to the base control functionality/specificity based on organizational assessments of risk.

SP 800-161 provides the following adapted version of AC-3:

- **Supplemental ICT SCRM Guidance:** Ensure that the information systems and the ICT supply chain infrastructure have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for ICT supply chain needs. Organizations should ensure a detailed definition of access enforcement.
- **Control enhancements:**

  (8) REVOCATION OF ACCESS AUTHORIZATIONS

  Supplemental ICT SCRM Guidance: Prompt revocation is critical to ensure that system integrators, suppliers, and external service providers who no longer require access are not able to access an organization's system. For example, in a "badge flipping" situation, a contract is

https://t.me/learningnets

transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the organization should retire the old credentials and issue completely new credentials.

(9) CONTROLLED RELEASE

Supplemental ICT SCRM Guidance: Information about the ICT supply chain should be controlled for release between the organizations. Information may be continuously exchanged between the organization and its system integrators, suppliers, and external service providers. Controlled release of organizational information provides protection to manage risks associated with disclosure.

As this example illustrates, each selected control from SP 800-53 is tailored to SCRM requirements by providing additional material. In addition, there is a new family of controls provided in SP 800-163 that does not appear in SP 800-53, known as *provenance controls*. SP 800-163 defines *provenance* as follows:

> For ICT SCRM, the records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to appropriate actors, functions, locales, or activities.

The concept of provenance relates to the fact that all systems and components originate at some point in the supply chain and can be changed throughout their existence. The recording of system and component origin along with the history of, the changes to, and the recording of who made the changes is called *provenance*. The three security controls in the SP 800-163 provenance family deal with creating and maintaining provenance within the ICT supply chain. The objective is to enable enterprise agencies to achieve greater traceability in the event of an adverse event, which is critical for understanding and mitigating risks. The three security controls in this family are:

- **Provenance policy and procedures:** Provides guidance for implementing a provenance policy.
- **Tracking provenance and developing a baseline:** Provides details concerning the tracking process.
- **Auditing roles responsible for provenance:** Indicates the role auditing plays in an effective provenance policy.

SCRM Best Practices

There a number of useful sources of guidance for best practices for SCRM, including the Information Security Forum's (ISF's) Standard of Good Practice for Information

https://t.me/learningnets

Security (SGP), NISTIR 7622, and the ISO 28000 series on supply chain security. The ISO series includes the following standards documents:

- ISO 28000, *Specification for Security Management Systems for the Supply Chain*
- ISO 28001, *Best Practices for Implementing Supply Chain Security, Assessments and Plans –Requirements and Guidance*
- ISO 28003, *Requirements for Bodies Providing Audit and Certification of Supply Chain Security Management Systems*
- ISO 28004, *Guidelines for the Implementation of ISO 28000*

At their SCRM website, the NIST lists practices adopted by companies for effective SCRM. One set of best practices deals with vendor selection and management and consists of the following:

- A focus on brand integrity rather than brand protection supports life cycle threat modeling, which proactively identifies and addresses vulnerabilities in the supply chain.
- Procurement and sourcing processes are developed jointly with input from IT, security, engineering, and operations personnel; sourcing decisions receive multi-stakeholder input.
- Standard security terms and conditions are included in all requests for proposals (RFPs) and contracts, tailored to the type of contract and business needs.
- Asset or business owners must formally accept responsibility for exceptions to security guidelines and any resulting business impact.
- Since many risk assessments depend on supplier self-evaluation, a number of companies employ onsite verification and validation of these reviews. Some companies cross-train personnel to be stationed at supplier companies so that security criteria are monitored year round.
- New suppliers enter a test and assessment period—to test the capabilities of the supplier and its compliance with various requirements—before they actively join the supply chain. In high-risk areas, for example, a supplier might go through a series of pilots before fully entering the supply chain.
- Tier 1 suppliers are required to give their suppliers the same survey that the original equipment manufacturer (OEM) requires of them.
- Approved vendor lists are established for manufacturing partners.
- Quarterly reviews of supplier performance are assessed among a stakeholder group.
- Annual supplier meetings ensure that suppliers understand the customers' business needs, concerns, and security priorities.

https://t.me/learningnets

- Mentoring and training programs are offered to suppliers, especially in difficult or key areas of concern to the company, such as cybersecurity.

For managing supply chain risk, companies should adopt the following practices:

- Security requirements are included in every RFP and contract.
- Once a vendor is accepted in the formal supply chain, a security team works with that vendor onsite to address any vulnerabilities and security gaps.
- Have a "one strike and you're out" policy with respect to vendor products that are either counterfeit or do not match specification.
- Component purchases are tightly controlled. For example, component purchases from approved vendors are prequalified, and parts purchased from other vendors are unpacked, inspected, and X-rayed before being accepted.
- Secure software life cycle development programs and training for all engineers in the life cycle are established.
- Source code is obtained for all purchased software.
- Software and hardware have a security handshake. Secure booting processes look for authentication codes, and the system will not boot if codes are not recognized.
- Automation of manufacturing and testing regimes reduces the risk of human intervention.
- Track-and-trace programs establish provenance of all parts, components, and systems.
- Programs capture "as built" component identity data for each assembly and automatically link the component identity data to sourcing information.
- Personnel in charge of supply chain cybersecurity partner with every team that touches any part of the product during its development life cycle and ensure that cybersecurity is part of suppliers' and developers' employee experience, processes, and tools.
- Legacy support is provided for end-of-life products and platforms to ensure a continued supply of authorized IP and parts.
- Tight controls are imposed on access by service vendors. Access to software is limited to a very few vendors. Hardware vendors are limited to mechanical systems and have no access to control systems. All vendors are authorized and escorted.

Supply chain risk management must be conducted as part of the overall risk management function in an organization. Thus, ultimately, a chief information security officer (CISO) or a person in a similar position is responsible for overseeing risk

https://t.me/learningnets

management and risk assessment for all the functions of an organization, including supply chain risk management.

13.3 Cloud Computing

There is an increasingly prominent trend in many organizations, known as *enterprise cloud computing*, that involves moving a substantial portion or even all IT operations to an Internet-connected infrastructure. This section provides an overview of cloud computing.

Cloud Computing Elements

NIST defines *cloud computing* in NIST SP-800-145, *The NIST Definition of Cloud Computing*, as follows:

> **Cloud computing:** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Figure 13.6 illustrates the relationships between the various models and characteristics mentioned in this definition.

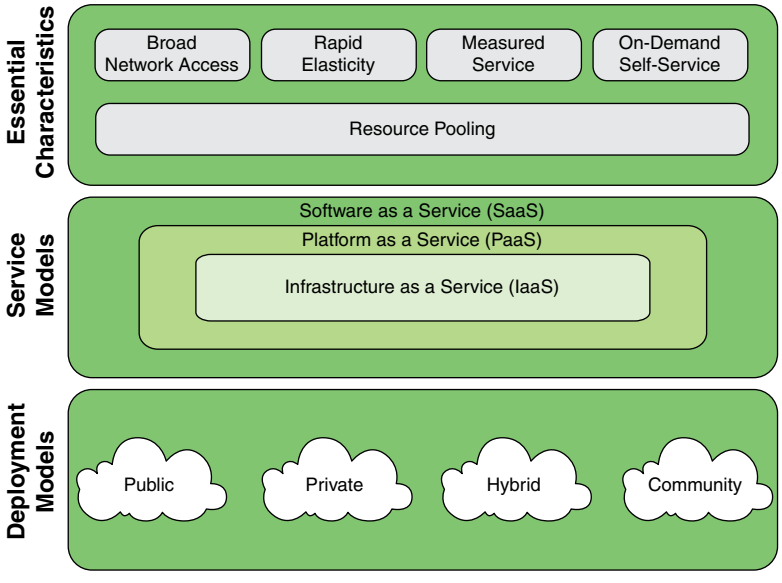


FIGURE 13.6 Cloud Computing Elements

https://t.me/learningnets

The essential characteristics of cloud computing include the following:

- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, laptops, and personal digital assistants (PDAs) as well as other traditional or cloud-based software services.
- **Rapid elasticity:** Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement. For example, you may need a large number of server resources only for the duration of a specific task. You want to be able to release those resources upon completion of the task.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, active user accounts). Resource usage is monitored, controlled, and reported, providing transparency for both the provider and the consumer of the utilized service.
- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Because the service is on demand, the resources are not permanent parts of the IT infrastructure.
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge of the exact location of the provided resources but may be able to specify location at a higher level of abstraction (for example, country, state, data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.

NIST defines three *service models*, which are viewed as nested service alternatives:

- **Software as a service (SaaS):** The consumer can use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service. SaaS eliminates the complexity of software installation, maintenance, upgrades,

https://t.me/learningnets

and patches. Examples of services at this level are Gmail, Google's email service, and Salesforce.com, which helps firms keep track of their customers.

- **Platform as a service (PaaS):** The consumer can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS often provides middleware-style services such as database and component services for use by applications. In effect, PaaS is an operating system in the cloud.
- **Infrastructure as a service (IaaS):** The consumer can provision processing, storage, networks, and other fundamental computing resources and can deploy and run arbitrary software, including operating systems and applications. IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems.

NIST defines four *deployment models*:

- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The cloud provider is responsible for both the cloud infrastructure and the control of data and operations within the cloud.
- **Private cloud:** The cloud infrastructure is operated solely for a single organization. It is either managed by the organization or a third party and exists on premises or off premises. The cloud provider is responsible only for the infrastructure and not for the control.
- **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community with shared concerns (for example, mission, security requirements, policy, compliance considerations). It is managed by the organizations or a third party and exists on premises or off premises.
- **Hybrid cloud:** The cloud infrastructure is a composite of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load balancing between clouds).

Figure 13.7 illustrates the two typical private cloud configurations. The private cloud consists of an interconnected collection of servers and data storage devices hosting enterprise applications and data. Local workstations have access to cloud resources from within the enterprise security perimeter. Remote users (for example, from satellite offices) have access through a secure link, such as a virtual private network (VPN) connecting to a secure boundary access controller, such as a firewall. An enterprise may also choose to outsource the private cloud to a cloud provider. The cloud

https://t.me/learningnets

provider establishes and maintains the private cloud, consisting of dedicated infrastructure resources not shared with other cloud provider clients. Typically, a secure link between boundary controllers provides communications between enterprise client systems and the private cloud. This link may be a dedicated leased line or a VPN over the Internet.

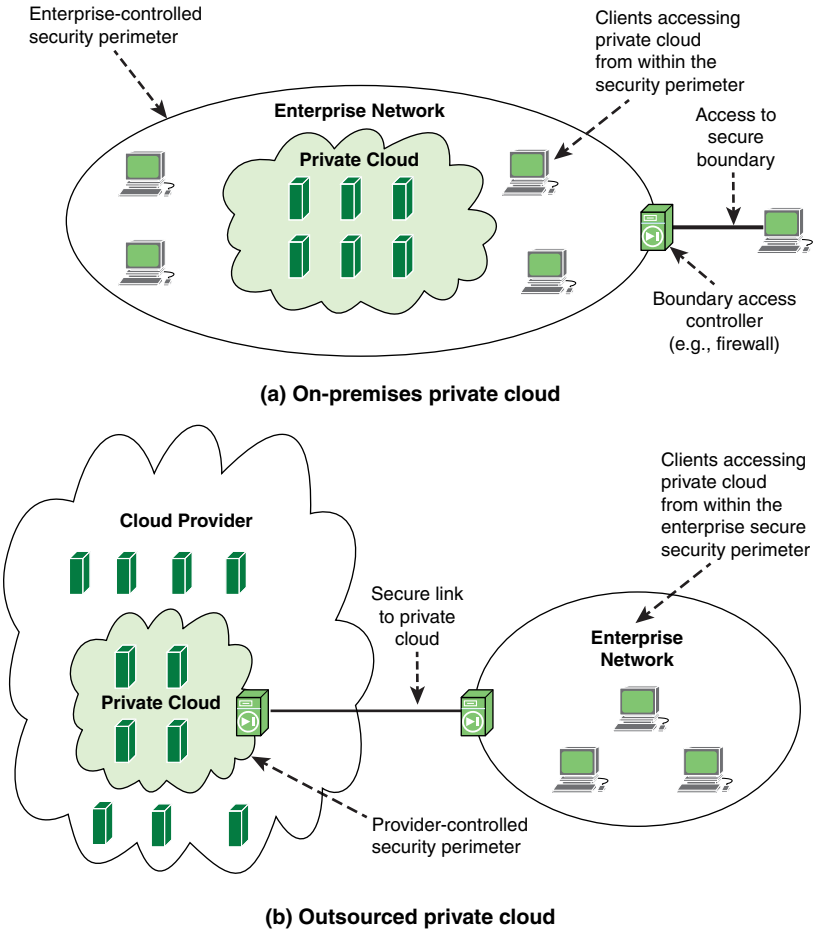


FIGURE 13.7 Private Cloud Configurations

Figure 13.8 shows a public cloud used to provide dedicated cloud services to an enterprise. The public cloud provider serves a diverse pool of clients. Any given enterprise's cloud resources are segregated from those used by other clients, but the degree of segregation varies among providers. For example, a provider dedicates a number of virtual machines to a given customer, but a virtual machine for one customer may share the same hardware as virtual machines for other customers.

https://t.me/learningnets

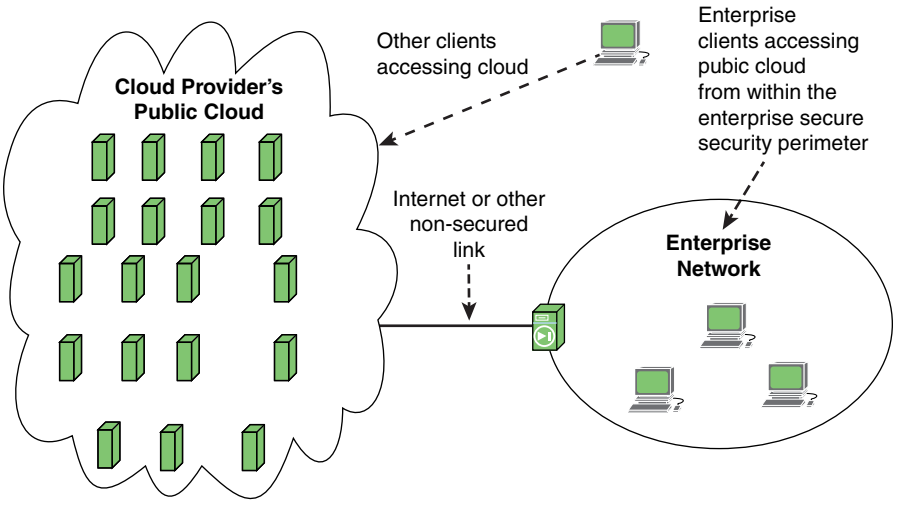


FIGURE 13.8 Public Cloud Configuration

Cloud Computing Reference Architecture

A cloud computing reference architecture depicts a generic high-level conceptual model for discussing the requirements, structures, and operations of cloud computing. NIST SP 500-292, *NIST Cloud Computing Reference Architecture*, establishes a reference architecture, described as follows:

> The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.

NIST developed the reference architecture with the following objectives in mind:

- To illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model
- To provide a technical reference for consumers to understand, discuss, categorize, and compare cloud services
- To facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations

https://t.me/learningnets

The reference architecture depicted in Figure 13.9 defines five major actors in terms of their roles and responsibilities:

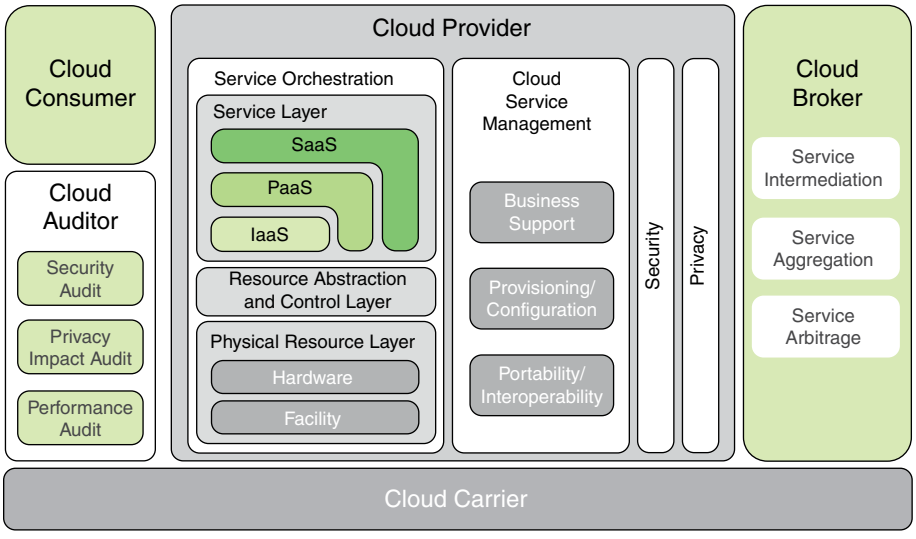


FIGURE 13.9 NIST Cloud Computing Reference Architecture

- **Cloud consumer:** A person or an organization that maintains a business relationship with, and uses services from, cloud providers
- **Cloud provider (CP):** A person, an organization, or an entity responsible for making a service available to interested parties
- **Cloud auditor:** A party that conducts independent assessment of cloud services, information system operations, performance, and security of the cloud implementation
- **Cloud broker:** An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between CPs and cloud consumers
- **Cloud carrier:** An intermediary that provides connectivity and transport of cloud services from CPs to cloud consumers

The roles of the cloud consumer and provider have already been discussed. To summarize, a *cloud provider*, or *cloud service provider* (*CSP*), provides one or more cloud services to meet the IT and business requirements of *cloud consumers*. For each of the three service models (SaaS, PaaS, and IaaS), the CP provides the storage

https://t.me/learningnets

and processing facilities needed to support that service model, together with a cloud interface for cloud service consumers. For SaaS, the CP deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers. The consumers of SaaS are organizations that provide their members with access to software applications, end users who directly use software applications, or software application administrators who configure applications for end users.

For PaaS, the CP manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components. Cloud consumers of PaaS use the tools and execution resources provided by CPs to develop, test, deploy, and manage the applications hosted in a cloud environment.

For IaaS, the CP acquires the physical computing resources underlying the service, including the servers, networks, storage, and hosting infrastructure. The IaaS cloud consumer in turn uses these computing resources, such as a virtual computer, for fundamental computing needs.

The *cloud carrier* is a networking facility that provides connectivity and transport of cloud services between cloud consumers and CPs. Typically, a CP sets up service level agreements (SLAs) with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers and can require the cloud carrier to provide dedicated and secure connections between cloud consumers and CPs.

A *cloud broker* is useful when cloud services are too complex for a cloud consumer to easily manage. Three areas of support are offered by a cloud broker:

- **Service intermediation:** These are value-added services, such as identity management, performance reporting, and enhanced security.
- **Service aggregation:** The broker combines multiple cloud services to meet consumer needs not specifically addressed by a single CP or to optimize performance or minimize cost.
- **Service arbitrage:** This is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

A *cloud auditor* evaluates the services provided by a CP in terms of security controls, privacy impact, performance, and so on. The auditor is an independent entity which ensures that the CP conforms to a set of standards.

https://t.me/learningnets

13.4 Cloud Security

This section focuses on cloud security from the point of view of a cloud consumer—that is, an organization that makes use of services from a cloud service provider.

Security Considerations for Cloud Computing

The following key issues that need to be addressed when an organization moves data and/or applications into the cloud:

- **Confidentiality and privacy:** An organization has commitments to its employees and customers in the areas of data confidentiality and privacy. Further, any breach of confidentiality or privacy can have adverse business impacts. Finally, regulations and legal restrictions apply. Placing data in the cloud introduces new risks that must be assessed.
- **Data breach responsibilities:** Placing data and services in the cloud amplifies concerns about data breaches, yet security is not under the direct control of the customer. The following are some issues in this regard:
  - **Responsibility for notifying:** Data breach generally carries with it an obligation to notify. Who is responsible for notification (customer, vendor, third party) and how quickly?
  - **Risks to intellectual property:** Risks include authorization, terms and conditions that (inappropriately) assert ownership over intellectual property held by third parties, and weakening of ability for organizations to assert "work made for hire" for creations that are developed "without use of organizational resources."
  - **Export controls:** Does the vendor house data at foreign sites? Are the systems managed by foreign nationals?
- **E-discovery:** Institutions and their legal counsel can be obligated to keep records needed for legal discovery. But these records are not under direct organizational control; the organization no longer has the record in the same way that it formerly did. How does one handle discovery in this externalized infrastructure?
- **Risk assessment:** To perform effective risk assessment, the customer must have considerable information about the security policies and controls in effect at the cloud service provider.
- **Business continuity:** Plans are needed to deal with the suspension or termination of the cloud service. The customer needs to have the portability capability to move data to a different cloud service provider.
- **Legal issues:** Legal risks and obligations must be clarified and documented.

https://t.me/learningnets

Threats for Cloud Service Users

The use of cloud services and resources introduces a novel set of threats to enterprise cybersecurity. For example, a report issued by the ITU-T [ITUT12] lists the following threats for cloud service users:

- **Responsibility ambiguity:** The enterprise-owned system relies on services from the cloud provider. The level of the service provided (SaaS, PaaS, IaaS) determines the magnitude of resources that are offloaded from IT systems on to the cloud systems. Regardless of the level of service, it is difficult to define precisely the security responsibilities of the customer and those of the cloud service provider. If there is any ambiguity, this complicates risk assessment, security control design, and incident response.
- **Loss of governance:** The migration of a part of the enterprises IT resources to the cloud infrastructure gives partial management control to the cloud service provider. The degree of loss of governance depends on the cloud service model (SaaS, PaaS, IaaS). In any case, the enterprise no longer has complete governance and control of IT operations.
- **Loss of trust:** It is sometimes difficult for a cloud service user to assess the provider's trust level due to the black-box feature of the cloud service. There is no way to obtain and share the provider's security level in a formalized manner. Furthermore, cloud service users are generally unable to evaluate the security implementation level achieved by the provider. This in turn makes it difficult for the customer to perform a realistic risk assessment.
- **Service provider lock-in:** A consequence of the loss of governance could be a lack of freedom in terms of how to replace one cloud provider with another. An example of a difficulty in transitioning is if a cloud provider relies on nonstandard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.
- **Nonsecure cloud service user access:** As most of the resource deliveries are through remote connections, unprotected application programming interfaces (APIs) (mostly management APIs and PaaS services) are among the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities pose significant threats.
- **Lack of asset management:** The cloud service user may have difficulty in assessing and monitoring asset management by the cloud service provider. Key elements of interest include location of sensitive asset/information, degree of physical control for data storage, reliability of data backup (data retention issues), and countermeasures for business continuity and disaster

https://t.me/learningnets

recovery. Furthermore, cloud service users are also likely to have important concerns about exposure of data to foreign governments and compliance with privacy laws.

- **Data loss and leakage:** This threat can be strongly related to the preceding item. However, loss of an encryption key or a privileged access code brings serious problems to cloud service users. Accordingly, lack of cryptographic management information, such as encryption keys, authentication codes, and access privilege, lead to sensitive damages, such as data loss and unexpected leakage to the outside.

Risk Evaluation

It is useful to have a detailed questionnaire for performing risk evaluation for cloud services. The Information Security Council developed a template to be used for this purpose [HEIS14b]. The template includes the questions in the following areas (the full document is available at this book's document resource site):



Cybersecurity Book Resource Site https://app.box.com/v/ws-cybersecurity

- High-level description
- Authentication
- Authorization—logical access control
- Data security
- Recoverability
- Operational controls
- Incident response
- Application security
- Testing and validation

The questionnaire is quite detailed. For example, the application security section includes the following questions:

8.0 APPLICATION SECURITY

8.1 Does the software development life-cycle model used by the hosting service provider in the development of their software, incorporate features from any standards based framework models (for example, TSP-Secure, SAMM, Microsoft SDL, OWASP, NIST SP800-64 rev 2,)? If so, please specify.

8.1.1 Are security components identified and represented during each phase of the software development life -cycle?

https://t.me/learningnets

8.2 Does the service provider have change management policies in place?

- **8.2.1** Is a pre-determined maintenance window used to apply changes?
- **8.2.2** How much lead-time will the service provider give customer of upcoming changes?
- **8.2.3** How are customers notified of changes?
- **8.2.4** Does the service provider have a process to test their software for anomalies when new operating system patches are applied?
- **8.2.5** Has a technical and/or security evaluation been completed or conducted when a significant change occurred?

8.3 Are source code audits performed regularly?

- **8.3.1** Are source code audits performed by someone other than the person or team that wrote the code?

8.4 Is access to the service provider's application restricted to encrypted channels (for example, https)?

8.5 Describe the session management processes used by the hosted service's applications.

During the proposal phase of contract procurement, the cloud service provider should be required to fill out this questionnaire. If the answers are satisfactory, they should be incorporate into the contract as provider commitments.

Best Practices

When using a public cloud or an outsourced private cloud, an enterprise is faced with a complex environment in which to evaluate threats, vulnerabilities, and risks. Much of the challenge relates to the adequacy of the cloud provider's security controls. Thus, the enterprise must exercise due diligence when selecting and moving functions and resources to a cloud. As a guide, SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, provides a list of best practices for outsourcing to a cloud service provider, in three categories:

- Preliminary activities:
  - Identify security, privacy, and other organizational requirements for cloud services to meet as a criterion for selecting a cloud provider.
  - Analyze the security and privacy controls of a cloud provider's environment and assess the level of risk involved with respect to the control objectives of the organization.

https://t.me/learningnets

- Evaluate the cloud provider's ability and commitment to deliver cloud services over the target time frame and meet the security and privacy levels stipulated.

- Initiating and coincident activities:
  - Ensure that all contractual requirements are explicitly recorded in the service agreement, including privacy and security provisions, and that they are endorsed by the cloud provider.
  - Involve a legal advisor in the review of the service agreement and in any negotiations about the terms of service.
  - Continually assess the performance of the cloud provider and the quality of the services provisioned to ensure that all contract obligations are being met and to manage and mitigate risk.
- Concluding activities:
  - Alert the cloud provider about any contractual requirements that must be observed upon termination.
  - Revoke all physical and electronic access rights assigned to the cloud provider and recover physical tokens and badges in a timely manner.
  - Ensure that organizational resources made available to or held by the cloud provider under the terms of service agreement are returned or recovered in a usable form and ensure that information has been properly expunged.

Cloud Service Agreement

From point of view of the overall mission and objectives of an enterprise—and in particular from the point of view of security—an essential aspect of using outsourced cloud services is a formal cloud service agreement (CSA). The Cloud Standards Customer Council list the following as the typical major components of a CSA [CSCC15]:



Cloud Standards Customer Council http://www.cloud-council.org

- **Customer agreement:** Describes the overall relationship between the customer and provider. Terms include how the customer is expected to use the service, methods of charging and paying, reasons a provider can suspend service, termination, and liability limitations.
- **Acceptable use policies:** Prohibits activities that providers consider to be an improper or illegal use of their service. In addition, the provider usually agrees not to violate the intellectual property rights of the customer.

https://t.me/learningnets

- **Cloud service level agreements:** Defines a set of service level objectives, including availability, performance, security, and compliance/privacy. The SLA specifies thresholds and financial penalties associated with violations of these thresholds. Well-designed SLAs significantly contribute to avoiding conflict and facilitate the resolution of issues before they escalate into disputes.
- **Privacy policies:** In general, the privacy policy describes the different types of information collected; how that information is used, disclosed, and shared; and how the provider protects that information. Portions of this agreement can define what information is collected about the customer, what personally identifiable information (PII) is to be stored, and the physical location information.

13.5 Supply Chain Best Practices

The SGP breaks down the best practices in the supply chain management category into two areas and four topics and provides detailed checklists for each topic. The areas and topics are:

- **External supplier management:** The objective of this area is to identify and manage information risk throughout each stage of relationships with external suppliers (including suppliers of hardware and software throughout the supply chain, outsourcing specialists, and cloud service providers) by embedding information security requirements in formal contracts and obtaining assurance that they are met.
  - **External supplier management process:** Describes procedures for identifying and managing information risks throughout all stages of the relationship with external suppliers (including organizations in the supply chain).
  - **Outsourcing:** Describes procedures for governing the selection and management of outsourcing providers (including cloud service providers), supported by documented agreements that specify the security requirements to be met.
- **Cloud computing:** The objective of this area is to establish and enforce a comprehensive cloud security policy, which specifies the need to incorporate specialized information security requirements in cloud-specific contracts and communicate it to all individuals who purchase or use cloud services.

https://t.me/learningnets

- **Cloud computing policy:** Defines the elements to be included in a policy on the use of cloud services, to be produced and communicated to all individuals who purchase or use cloud services.
- **Cloud service contracts:** Provides a detailed list of obligations on the part of the cloud service provider to be included in the service contract.

13.6 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

cloud auditor
cloud broker
cloud carrier
cloud computing
cloud consumer
cloud provider
community cloud
exfiltration
hybrid cloud
ICT supply chain
information and communications technology (ICT)
infrastructure as a service (IaaS)
intellectual property rights (IPR)
key performance indicators (KPIs)
platform as a service (PaaS)
private cloud
public cloud
provenance
software as a service (SaaS)
supply chain
supply chain management
supply chain risk management (SCRM)

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. What does ICT stand for, and what does it mean?
2. Explain the concept of a supply chain. How is an ICT supply chain different from a general supply chain?
3. Explain three types of flows associated with a supply chain.
4. Describe key elements involved in supply chain management.
5. What are the three tiers of risk management defined in SP 800-161?
6. What are the main external risks of a supply chain?

https://t.me/learningnets

7. What are the main internal risks of a supply chain?
8. List the supply chain security controls mentioned in SP 800-161 standard.
9. Enumerate three security controls in the provenance family.
10. Define the term *cloud computing*.
11. What are key characteristics of cloud computing?
12. What are the three service models of cloud computing, according to NIST?
13. Describe the cloud deployment models included in the NIST standard.
14. What are the central elements in NIST's cloud computing reference architecture?
15. What are some of the threats for cloud service users?
16. What are the key components of a cloud service agreement, according to the Cloud Standards Customer Council?

13.7 References

CSCC15: Cloud Standards Customer Council, *Practical Guide to Cloud Service Agreements.* April 2015. http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

HEIS14b: Higher Education Information Security Council, "Cloud Computing Security." *Information Security Guide*, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Cloud+Computing+Security

ITUT12: ITU-T, *Focus Group on Cloud Computing Technical Report Part 5: Cloud Security*. FG Cloud TR, February 2012.

WILD13: Wilding, R., "Classification of the Sources of Supply Chain Risk and Vulnerability." August 2013. http://www.richardwilding.info/blog/the-sources-of-supply-chain-risk

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Chapter 14

Technical Security Management

"I am fairly familiar with all the forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers," said Holmes.

—*The Adventure of the Dancing Men*, Sir Arthur Conan Doyle

Learning Objectives

After studying this chapter, you should be able to:

- Explain the purpose and key characteristics of a security architecture.
- Discuss malware protection strategies.
- Understand the requirements for malware protection software.
- Present an overview of identity and access management concepts.
- Describe the principal approaches to intrusion detection.
- Explain the key elements in a data loss prevention solution.
- Understand the basic concepts of digital rights management.
- Explain the key requirements for effective implementation and use of cryptographic algorithms.
- Discuss the nature of public key infrastructure.
- Present an overview of technical security management best practices.

The term *technical security* is often used to contrast software- and hardware-based security controls with management and operational security controls. *Technical security management* refers to the overall development of a management plan and policies to effectively manage the design, implementation and evaluation of technical security controls. For example, the use of virtual private networks

https://t.me/learningnets

and firewalls are **technical security controls**; training employees in acceptable use policies, security auditing, and the development of a security governance structure are nontechnical security controls.

technical security controls
Security controls (that is, safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) divides technical security management into two main areas: security solutions and cryptography. With respect to security solutions, the SGP addresses the need for an overall security architecture to provide a framework for technical security control development and then details policies and procedures in specific technical areas (see Sections 14.1 through 14.7). For a detailed technical discussion of these topics, see Stallings and Brown's *Computer Security: Principles and Practice* [STAL18].

With respect to cryptography, the SGP is concerned with developing management guidelines for the choice and use of cryptographic algorithms, for cryptographic key management, and for implementing a public key infrastructure (see Sections 14.8 through 14.10). For a detailed technical discussion of these topics, see *Cryptography and Network Security* by Stallings [STAL17].

14.1 Security Architecture

A security architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible. In a security architecture, the design principles are reported clearly, and in-depth security control specifications are generally documented in independent documents. A security architecture can be considered a design that includes a structure and addresses the connection between the components of that structure.

A security architecture is a prescriptive document that uses a set of coherent models and principles to guide the implementation of the information security policy of an organization. A security architecture has the following key characteristics:

- It consists of a transparent and coherent overview of models, principles, starting points, and conditions that give a concrete interpretation of the information security policy, usually without speaking in terms of specific solutions.
- It reduces a complex problem into models, principles, and subproblems to be understood.
- The models and principles show where you take which type of measures, when the principles are applicable, and how they connect with other principles.

https://t.me/learningnets

The SABSA Institute http://www.sabsa.org

One of the most widely used security architectures is the Sherwood Applied Business Security Architecture (SABSA) Enterprise Security Architecture [SHER09]. SABSA was developed to provide an end-to-end framework for determining, designing, and deploying security in a way that is traceably aligned with the business and into which the many traditional standards and processes can be incorporated. It is now widely recognized as the leading methodology for developing business operational risk-based architectures in general [BURK12, SHOR10]. SABSA takes a carefully designed and business-focused path from eliciting key business service requirements through to identifying the security architecture, services, mechanisms, and components needed to support the business while also addressing service management.

The SABSA model consists of five hierarchical layers, with a sixth layer spanning the other five (see Figure 14.1):

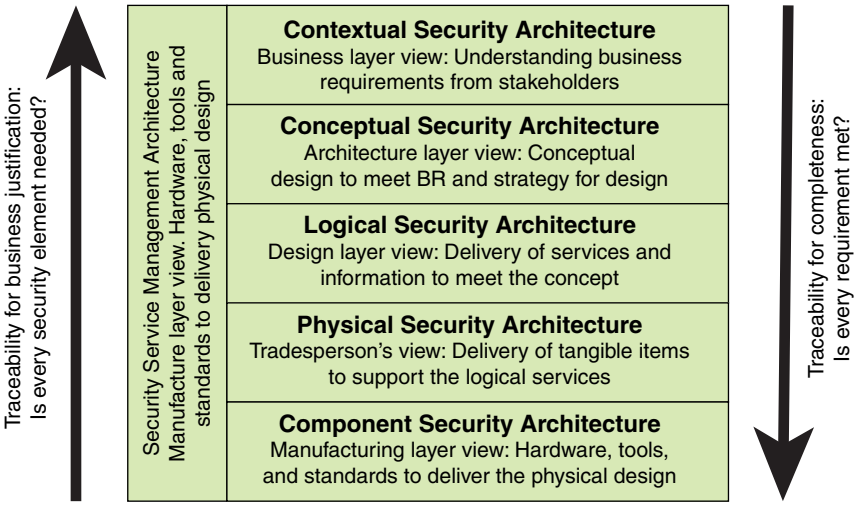


FIGURE 14.1 The SABSA Model for Security Architecture

- **Contextual security architecture:** This layer describes the key business issues, starting with the assets, the motivation for providing security, the business processes, the organization, geographic dispersion, and key time-related considerations in these processes. Business drivers—the desired outcomes for the business—are assets at the contextual layer, and they are determined from various sources, such as interviews and plans. The motivation for security is determined by looking at what regulations or risk factors are associated with the business drivers, and the business processes can be described.

https://t.me/learningnets

- **Conceptual security architecture:** The security characteristics of each of the business drivers are considered at the conceptual layer. For this purpose, an organization may use the SABSA information and communications technology (ICT) Business Attribute Taxonomy, a set of attributes described in business language that reflect security characteristics. The standard taxonomy has 53 such attributes, including the traditional security attributes confidentiality, availability, and integrity. By associating a set of these attributes with each business driver, you can define a security architecture in a way that provides full traceability back to business needs. At this layer, the security domains and associated policy architecture are defined, both of which are key to defining ownership so that correct security governance is applied. The architectural strategies are also defined in this layer—specifically, the risk/control strategy and compliance framework and the SABSA multitiered approach of deterrence, prevention, containment, detection, and recovery/restoration. Security performance and service level agreements (SLAs) are also defined at the conceptual layer.
- **Logical security architecture:** This layer provides a design layer view, focusing on the delivery of services and information to meet the security concept.
- **Physical security architecture:** This layer deals with the delivery of tangible items to support the logical services.
- **Component security architecture:** This layer defines the hardware and tools to deliver the physical design and provides a mapping to conform to standards.
- **Security service management architecture:** This layer addresses issues related to how the organization manages the architecture.

The most powerful tools in the SABSA architecture are attributes and attribute profiling. Attributes provide a conceptualized and normalized way of describing a business driver (a security-focused version of a business requirement). Normally one, two, or three words make up an attribute, such as *available* or *access controlled*, and the attribute is assigned to a business driver (which supports a business requirement). Attributes are used to tag aspects of the architectural design to allow two-way traceability up and down the layers to provide transparent traceability to the stakeholders and to understand the controls that support the various business requirements.

An important guide to the use of SABSA is the SABSA security architecture matrix, shown in Table 14.1. Each row corresponds to one of the six layers of the architecture. The six columns define the key questions that need to be addressed at each level (what,

https://t.me/learningnets

TABLE 14.1 The SABSA Matrix for Security Architecture

SABSA Layer	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business time dependence
Conceptual	Risk strategy	Control objectives	Security strategies	Roles and responsibilities	Security domain	Time management
Logical	Information assets	Risk management policies	Security services	Privilege profiles	Domain maps	Calendar and timetable
Physical	Data assets	Risk management practices	Security mechanisms	User interface	ICT infrastructure	Processing schedule
Component	ICT components	Security standards	Security products/tools	Identities and functions	Locator tools and standards	Timers and interrupts
Service Management	Service delivery management	Operational risk management	Process delivery management	Personnel management	Management of the environment	Time/ performance management

https://t.me/learningnets

why, how, who, where, and when). If an organization addresses the issues raised by each and every one of these cells, then it has covered the entire range of questions to be answered and can have a high level of confidence that the security architecture is complete. The SABSA process of developing enterprise security architecture is a process of populating all 36 of these cells.

The matrix also provides two-way traceability, as shown in Figure 14.1:

- **Completeness:** Has every business requirement been met? The layers and matrix allow you to trace every requirement through to the components that provide a solution.
- **Justification:** Is every component of the architecture needed? When someone asks "Why are you doing it this way?" the rationale is plain if you trace back to the business requirements that drive the specific solution.

14.2 Malware Protection Activities

malicious software (malware)
Software that exploits vulnerabilities in a computing system to create an attack.

Malicious software (malware) is perhaps the most significant security threat to organizations. National Institute of Standards and Technology (NIST) SP 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, defines *malware* as follows:

> **malware:** A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Hence, malware can pose a threat to application programs, to utility programs (such as editors and compilers), and to kernel-level programs. Malware is also used on compromised or malicious websites and servers, or in especially crafted spam emails or other messages, which aim to trick users into revealing sensitive personal information.

This section begins with a brief survey of types of malware and then discusses best practices for malware protection.

Types of Malware

Although the terminology related to malware is not consistent, the following list provides a useful guide to the various types of malware:

- **Adware:** Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

https://t.me/learningnets

- **Auto-rooter:** A malicious hacker tool used to break in to new machines remotely.
- **Backdoor (trapdoor):** Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality.
- **Exploit:** Code specific to a single vulnerability or set of vulnerabilities.
- **Downloader:** A program that installs other items on a machine that is under attack. Usually, a downloader is sent in an email message.
- **Dropper:** A malware installer that surreptitiously carries viruses, backdoors, and other malicious software to be executed on the compromised machine. Droppers don't cause harm directly but deliver a malware payload onto a target machine without detection.
- **Polymorphic dropper:** Also called a polymorphic packer, a software exploit tool that bundles several types of malware into a single package, such as an email attachment, and can force its "signature" to mutate over time, making it difficult to detect and remove.
- **Flooder:** A tool used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
- **Keyloggers:** A software tool that captures keystrokes on a compromised system.
- **Kit (virus generator):** A set of tools for generating new viruses automatically.
- **Logic bomb:** A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met, at which point the program triggers an unauthorized act.
- **Malware as a Service (MaaS):** A web-based provider of malware. MaaS may provide access to botnets, support hotlines, and servers that regularly update and test malware strains for efficacy.
- **Mobile code:** Software (for example, script, macro, or other portable instructions) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
- **Potentially unwanted program (PUP):** A program that may be unwanted, despite the possibility that users consented to download it. PUPs include spyware, adware, and dialers and are often downloaded in conjunction with programs that users actually want.

https://t.me/learningnets

- **Ransomware:** A type of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.
- **Remote access Trojan (RAT):** A malware program that includes a back-door for administrative control over the target computer. RATs are usually downloaded invisibly with user-requested programs—such as games—or sent as email attachments.
- **Rootkit:** A set of hacker tools used after attacker has broken into a computer system and gained root-level access.
- **Scraper:** A simple program that searches a computer's memory for sequences of data that match particular patterns, such as credit card numbers. Point-of-sale terminals and other computers usually encrypt payment card data when storing and transmitting it, and attackers often use scrapers to locate card numbers in memory before they are encrypted or after they are decrypted for processing.
- **Spammer programs:** Programs used to send large volumes of unwanted email.
- **Spyware:** Software that collects information from a computer and transmits it to another system.
- **Trojan horse:** A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
- **Virus:** Malware that, when executed, tries to replicate itself into other executable code; when it succeeds, the code is infected. When the infected code is executed, the virus also executes.
- **Web drive-by:** An attack that infects a user system when the user visits a web page.
- **Worm:** A computer program that runs independently and propagates a complete working version of itself onto other hosts on a network.
- **Zombie, bot:** A program that is activated on an infected machine to launch attacks on other machines.

https://t.me/learningnets

The Nature of the Malware Threat

The European Union Agency for Network and Information Security's annual threat report [ENIS18] lists malware as the top cyber threat for 2016 and 2017. Key findings of the report include the following:

- Businesses experienced far more malware threats in 2017 compared to 2016.
- Ransomware continues to dominate the Windows malware scene, with an evolution from 55% in January 2017 to 75% in July 2017.
- There is increasing threat from **clickless malware**, which is automated malware injection programs that do not require user action to activate.
- There is also a rise in **fileless malware**, which is malware code that resides in RAM (random access memory) or propagates through the use of carefully crafted scripts, such as PowerShell, to infect its host.
- There has been a growth of malicious functions being packaged within **Potentially Unwanted Programs (PUPs)**. While legitimate browser developers like Firefox and Chrome are making efforts to tighten security, the adware industry is creating its own custom browsers without any built-in security features and bundling them along with adware applications. They will replace your own browser as the default browser and expose you to the greater risks of using such a browser.

Practical Malware Protection

The battle against malware is never-ending. It is an ongoing arms race between malware producers and defenders. As effective countermeasures are developed for existing malware threats, newer types and modifications of existing types are developed. Malware enters through a variety of attack surfaces, including end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Malware is designed to avoid, attack, or disable defenses. And malware is constantly evolving to stay ahead of existing defenses.

Given the complexity of the challenge, organizations need to automate anti-malware actions as much as possible. Figure 14.2, based on one in the Center for Internet Security's *The CIS Critical Security Controls for Effective Cyber Defense* [CIS18}, indicates typical elements. Effective malware protection must be deployed at multiple potential points of attack. Enterprise endpoint security suites should provide administrative features to verify that all defenses are active and current on every managed system. There should be systems in place to collect ongoing incident results, with appropriate analysis and automated corrective action.

https://t.me/learningnets

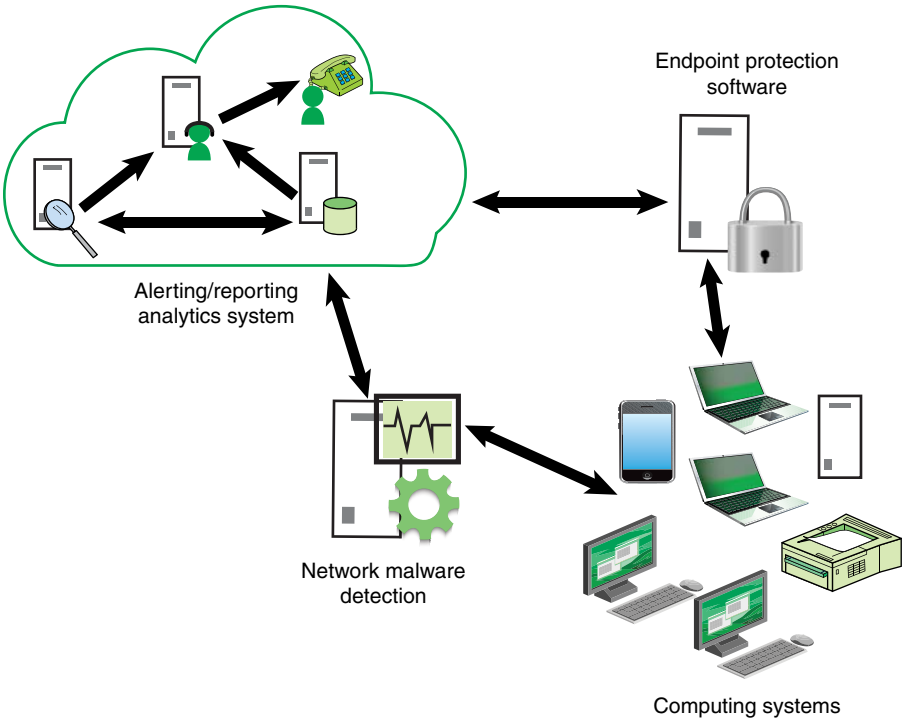


FIGURE 14.2 Malware System Entity Relationship Diagram

IT management can take a number of practical steps to provide the best possible protection at any given time, including the following:

1. Define procedures and responsibilities to deal with malware protection on systems, including training in their use, reporting, and recovering from malware attacks.
2. Where practical, do not grant administrative or root/superuser privileges to end users to limit the damage done by malware to gain the status of an authenticated user on a system.
3. Have a system and policies in place to keep track of where sensitive data is located, to erase data when no longer needed, and to concentrate security resources on systems that contain sensitive data. Section 14.6 elaborates on this topic.
4. Conduct regular reviews of the software and data content of systems supporting critical business processes; formally investigate the presence of any unapproved files or unauthorized amendments.

https://t.me/learningnets

5. Ensure that user and server platforms are well managed, especially Windows platforms, which continue to be a major target. Tasks include:
   - Install security updates as soon as available. Patch management software and outsourced services help in this regard.
   - Enforce password selection policies to prevent password-guessing malware from infecting systems.
   - Monitor systems for new unexplained listening network ports.
6. Key staff (for example, information security specialists, IT personnel responsible for system and application software) should regularly participate in security training and awareness events that cover malware.
7. Establish a formal policy (as part of acceptable use policy) prohibiting the use of unauthorized software.
8. Install and appropriately maintain endpoint defenses, including the following:
   - Use centrally managed antivirus and anti-spyware software where appropriate. An example is Microsoft System Center Endpoint Protection.
   - Enable and appropriately configure host-based firewalls where practical.
   - Enable and appropriately configure host-based intrusion prevention where practical.
   - Where feasible, make available protection software that is licensed for personal use.
9. Use Domain Name System (DNS)–based protection where practicable. A particular type of malware allows attackers to hijack the DNS settings of PCs, home gateways, and applications. Hijacking these settings allows an attacker to launch man-in-the-middle attacks against DNS transactions. These attacks overwrite DNS settings located on the subscriber's computer or home gateway to new fraudulent or malicious targets. This change effectively allows the attacker to take over (hijack) traffic for the unsuspecting Internet broadband consumer [MAAW10].
10. Use web filtering software, services, or appliances where practical. Examples of useful tools are the free Squid caching proxy, Forcepoint Web Security, and Microsoft Forefront Threat Management Gateway.
11. Implement application whitelisting where practical to allow systems to run software only if it is included on the whitelist and prevent execution of all other software on the system.



Squid
http://www.squid-cache.org

https://t.me/learningnets

12. Implement controls that prevent or detect the use of known or suspected malicious websites (for example, blacklisting).
13. Employ software or services that enable you to know where you are vulnerable. Examples are Nmap, which is open source, and Metasploit, which has open source and commercial versions. Commercial tools include Nessus and Rapid7.
14. Gather vulnerability and threat information from online sources, as discussed in Chapter 3, "Information Risk Assessment." Additional resources include:
    - Google's hostmaster tools to scan your sites and report malware
    - DShield, a service of the Internet Storm Center that provides a variety of tools
15. Monitor available logs and network activity for indicators of malicious software. This includes:
    - Regularly check antivirus logs.
    - Regularly check DNS traffic for queries to known malware hosting domains.
    - Centralize event log management and apply appropriate logic to identify out-of-spec results. An example of a tool that facilitates this is Microsoft System Center Operations Manager.
    - Subscribe to Shadowserver notifications for networks you manage. The Shadowserver Foundation is an all-volunteer, nonprofit, vendor-neutral organization that gathers, tracks, and reports on malicious software, botnet activity, and electronic fraud. It discovers the presence of compromised servers, malicious attackers, and the spread of malicious software. This reporting service is provided free of charge and is designed for organizations that directly own or control network space. It allows them to receive customized reports detailing detected malicious activity to assist in their detection and mitigation programs.
16. Have a backup strategy for your systems, including PCs, servers, and data storage devices. Ensure that the backup stream is encrypted over the Internet and enterprise networks.
17. Enable employees to report problems to IT security. In this regard, useful measures are:
    - All relevant points of contact should have current information in whois. This is an Internet program that allows users to query a database of people and other Internet entities, such as domains, networks, and hosts.



Nmap
https://nmap.org



Metasploit
https://www.metasploit.com



Google Malware Infection Resources
https://support.google.com/webmasters/answer/163635?hl=en



DShield Tools
https://secure.dshield.org/tools/

https://t.me/learningnets



Shadowserver http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

The information stored includes a person's company name, address, phone number, and email address

- Use standard abuse reporting addresses, as specified in RFC 2142, *Mailbox Names for Common Services, Roles and Functions*.
- Make sure your domain or domains are available at the Network Abuse Clearinghouse, which enables targets to report the origin of an unwanted message.

The preceding list includes recommendations from ISO 27002, *Code of Practice for Information Security Controls*, the SGP, the Payment Card Industry Data Security Standard (PCI DSS), and COBIT 5. The list also includes additional recommendations.



Whois https://www.whois.net

14.3 Malware Protection Software

The term *malware protection software* refers to automated tools used to mitigate threats from a broad range of ever-evolving malware. This section first examines the types of capabilities that are desirable in malware protection software and then examines management issues.



Network Abuse Clearinghouse https://www.abuse.net

Capabilities of Malware Protection Software

There are numerous open source and commercial malware protection software packages available for enterprise use, and most of them have similar capabilities. SP 800-83 lists the following as desired capabilities in malware protection software:

- Scanning critical host components such as startup files and boot records.
- Watching real-time activities on hosts to check for suspicious activity; a common example is scanning all email attachments for known malware as emails are sent and received. Configure anti-malware software to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as *on-access scanning*.
- Monitoring the behavior of common applications, such as email clients, web browsers, and instant messaging software. Monitor activity involving the applications most likely to be used to infect hosts or spread malware to other hosts with anti-malware software.
- Scanning files for known malware. Configure anti-malware software on hosts to scan all hard drives regularly to identify any file system infections and, optionally, depending on organization security needs, to scan removable media inserted into the host before allowing its use. Users should also be able to launch a scan manually as needed, which is known as *on-demand scanning*.

https://t.me/learningnets

- Identifying common types of malware as well as attacker tools.
- *Disinfecting* files, which refers to removing malware from within a file, and *quarantining* files, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed, and the original file restored; however, many infected files cannot be disinfected. Accordingly, configure anti-malware software to attempt to disinfect infected files and to either quarantine or delete files that cannot be disinfected.

Malware protection software does not provide the same level of protection against previously unknown viruses or other malware as it does against known threats and attack signatures. Accordingly, you should also have in place other measures, including:

- Application sandboxing, as discussed in Chapter 8, "System Development"
- Intrusion detection software to scan for anomalous behavior
- Awareness training that provides guidance to users on malware incident prevention
- Firewalls that by default deny unexpected behavior patterns
- Application whitelisting to prevent intrusion of unknown software
- Virtualization and container techniques to segregate applications or operating systems from each other

Managing Malware Protection Software

With any form of software that is installed on enterprise systems, you should have specific management policies for the life cycle of the software. Management policy should dictate the following measures for managing malware protection software:

- Document procedures for selecting, installing, configuring, updating, and reviewing malware protection software.
- Deploy the software on all systems exposed to malware, including those that are connected to networks or the Internet, support the use of portable storage devices, or are accessed by multiple external suppliers.
- Ensure that the installed suite of malware protection software protects against all forms of malware.
- Maintain a schedule for automatic and timely distribution of malware protection software.

https://t.me/learningnets

- Configure malware protection software to be active at all times, provide notification when suspected malware is detected, and remove malware and any associated files immediately upon detection.
- Review devices regularly to ensure that designated malware protection software is installed, enabled, and configured properly.

14.4 Identity and Access Management

The SGP defines identity and access management (IAM) as follows:

> **Identity and access management (IAM)** typically consists of several discrete activities that follow the stages of a user's life cycle within the organization. These activities fall into two categories:
>
> - Provisioning process, which provides users with the accounts and access rights they require to access systems and applications
> - User access process, which manages the actions performed each time a user attempts to access a new system, such as authentication and sign-on.

IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is increasingly business aligned and requires business skills, not just technical expertise. Enterprises that develop mature IAM capabilities reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

There are three deployment approaches for IAM:

- **Centralized:** All access decisions, provisioning, management, and technology are concentrated in a single physical or virtual location. Policies, standards, and operations are pushed out from this single location.
- **Decentralized:** Local, regional, or business units make the decisions for all access choices, provisioning, management, and technology. There may be enterprisewide policies and standards, but they provide guidance for the decentralized providers.
- **Federated:** Each organization subscribes to a common set of policies, standards, and procedures for the provisioning and management of users. Alternatively, the organizations can buy a service from a supplier.

https://t.me/learningnets

IAM Architecture

An architecture for identity and access management is a high-level model depicting the main elements and interrelationships of the IAM system. Figure 14.3 shows a typical architecture for an IAM system, whether centralized or decentralized.

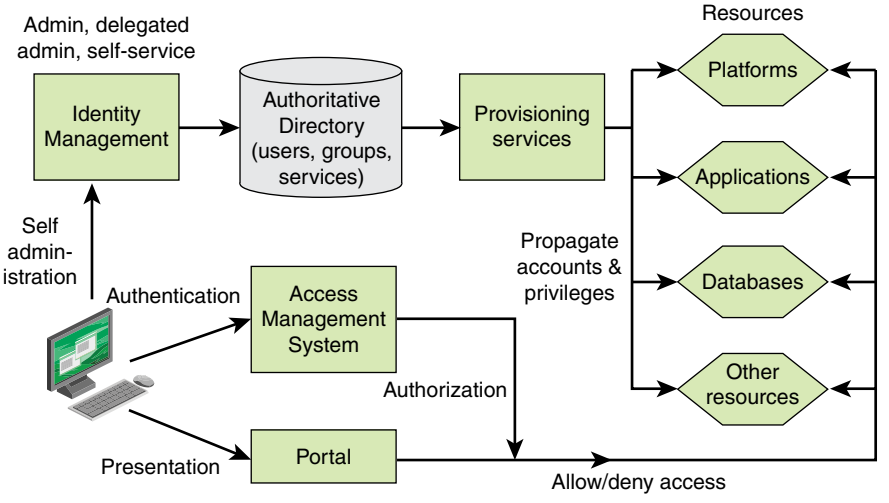


FIGURE 14.3 Identity and Access Management Infrastructure

Figure 14.3 includes the following elements:

- **Identity management service:** Defines an identity for each user (human or process), associates attributes with the identity, and enforces a means by which a user verifies identity. The central concept of an identity management system is the use of **single sign-on (SSO)**. SSO enables a user to access all network resources after a single authentication. The service implements facilities to enable user registration, changes in the user's status or other details, and deregistration. Identity management enables creation, deletion, or modification of the user profile and change of the user's role or association with a function, a business unit, or an organization.
- **Directory:** Provides a central identity repository and reconciliation of identity details between application-specific directories. Some items to be stored for each user include the following:
  - User credentials, such as user ID, password, and possibly certificates to enable authentication
  - Attributes, such as roles and groups that form a basis for authorization

single sign-on (SSO)
A security subsystem that enables a user identity to be authenticated at an identity provider—that is, at a service that authenticates and asserts the user's identity—and then have that authentication be honored by other service providers.

https://t.me/learningnets

- User preferences to enable personalization
- An access control policy that defines access permissions for distinctive data entries

- **Access management system:** Implements user authentication.
- **Portal:** Provides a personalized interface for all user interaction with system resources.
- **Provisioning services:** Covers centralized user administration capabilities. Provisioning services serve to automate the task of changing users' rights and privileges across multiple enterprise applications. They enable fast creation of new employee accounts and augment existing security practices by allowing administrators to quickly cut off terminated accounts.

Federated Identity Management

Federated identity management refers to the agreements, standards, and technologies that enable the portability of identities, identity attributes, and entitlements across multiple enterprises and numerous applications and supporting many thousands—or even millions—of users. When multiple organizations implement interoperable federated identity schemes, an employee in one organization uses SSO to access services across the federation, via trust relationships associated with the identity. For example, an employee may log on to her corporate intranet and be authenticated to perform authorized functions and access authorized services on that intranet. The employee could then access her health benefits from an outside health care provider without having to re-authenticate.

Beyond SSO, federated identity management provides other capabilities. One is a standardized means of representing attributes. Increasingly, digital identities incorporate attributes other than simply an identifier and authentication information (such as passwords and biometric information). Examples of attributes include account numbers, organizational roles, physical location, and file ownership. A user may have multiple identifiers—perhaps associated with multiple roles—each with its own access permissions.

Another key function of federated identity management is identity mapping. Different security domains may represent identities and attributes differently. Further, the amount of information associated with an individual in one domain may be more than is necessary in another domain. The federated identity management protocols map identities and attributes of a user in one domain to the requirements of another domain.

https://t.me/learningnets

Figure 14.4 illustrates entities and data flows in a generic federated identity management architecture.

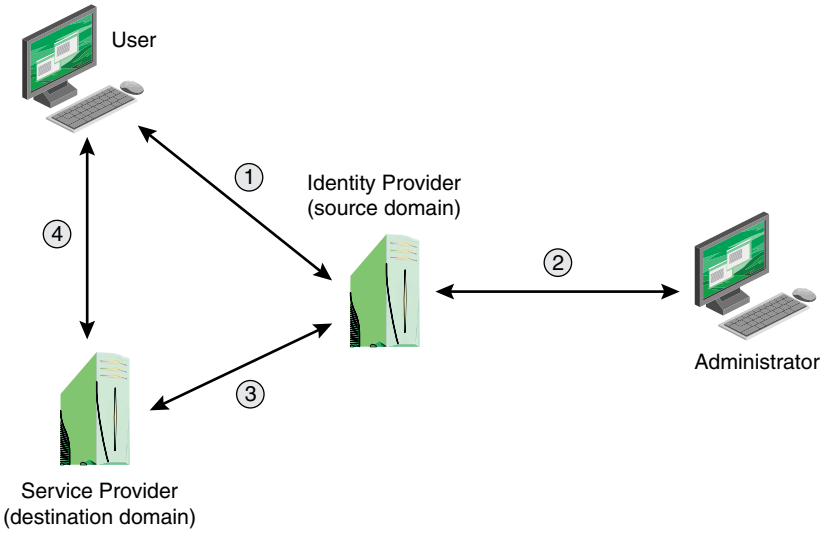


FIGURE 14.4 Federated Identity Operation

The numbered links in Figure 14.4 indicate the following actions:

1. The end user's browser or other application engages in an authentication dialogue with an identity provider in the same domain. The end user also provides attribute values associated with the user's identity.
2. Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.
3. A service provider in a remote domain that the user wishes to access obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.
4. The service provider opens a session with a remote user and enforces access control restrictions based on the user's identity and attributes.

The identity provider acquires attribute information through dialogue and protocol exchanges with users and administrators. For example, a user needs to provide a shipping address each time an order is placed with a new web merchant, and this information needs to be revised when the user moves. Identity management enables the user to provide this information once, so that it is maintained in a single place and released to data consumers in accordance with authorization and privacy policies.

https://t.me/learningnets

Service providers are entities that obtain and employ data maintained and provided by identity providers, often to support authorization decisions and to collect audit information. For example, a database server or file server is a data consumer that needs a client's credentials in order to know what access to provide to that client. A service provider can be in the same domain as the user and the identity provider. The power of this approach is for federated identity management, in which the service provider is in a different domain (for example a vendor or supplier network).

The goal is to share digital identities so a user is authenticated once and then can access applications and resources across multiple domains, such as autonomous internal business units, external business partners, and other third-party applications and services. The cooperating organizations form a federation based on agreed standards and mutual levels of trust to securely share digital identities. Federated identity management reduces the number of authentications needed by a user.

IAM Planning

Given the complexity of IAM, a sound planning process is needed to produce a cost-effective solution. The following process, based on the Higher Education Information Security Council's article "Identity and Access Management" [HEIS14c], suggests a comprehensive planning process:

1. Define the challenge and the approach to meet it. Clearly understand and articulate the institution's IAM desired state, target services, target users, and impacted functions (for example, SSO, two-factor, federation, automation of IAM processes). Define the approach needed to meet the challenge (including a high-level description of policies, technology, and business processes that need to be addressed).
2. Define the business and regulatory drivers and their importance to the institution's missions.
3. Define and document the enterprise's current IAM posture.
    - Does the enterprise have policies for IAM in place?
    - What is the institution's IAM and policy governance approach?
    - What is the degree of centralization? Are authentication decisions made by system, by application, by department, or centralized?
    - How are identifiers and credentials issued to users? Is the provisioning process consistent throughout the enterprise? Does it involve in-person vetting? Is self-service capability available for password resets?
    - Are authentication requirements for applications and services risk based?

https://t.me/learningnets

4. Determine the gaps between the enterprise's current IAM posture and the desired state, target services, and target users.
    - Map a matrix of the target users and target services and determine the required policies, processes, and technology, considering the risk and the business and regulatory requirements.
5. Identify project stakeholders and determine who should be involved and the level and timing of their involvement.
6. Develop the policy framework.
    - What are the roles and responsibilities?
    - What is required to identify users?
    - What criteria are used to determine the types of credentials used?
    - What criteria are used to determine the level of access to applications and services?
    - What is required from identity providers and from service providers?
7. Develop the required business processes. What steps are required to:
    - Identify and register a user?
    - Provision and deprovision credentials?
    - Provide support and training?
    - Request, grant, and modify access to applications and services?
8. Develop the technology framework.
    - Specify the source of authority systems.
    - Indicate the authentication protocols and technologies.
    - List approaches and products.
    - Enumerate staff and skill sets.

IAM Best Practices

Andy Zindel's blog post "IAM Best Practices to Reduce Your Attack Surface" [ZIND17] provides a list of best practices for avoiding common security mistakes with IAM, based on experience by Verizon and Centrify, a security services firm:

- **Make people your first line of defense:** Train staff to spot the warning signs of phishing attacks and social engineering.
- **Patch promptly and completely:** This helps guard against many attacks.

https://t.me/learningnets

- **Encrypt sensitive data:** Make your data next to useless if it is stolen.
- **Use multifactor authentication (MFA):** Limit the damage that can be done with lost or stolen credentials.
- **Implement least-privilege access controls:** Make sure that only staff who need access to systems to do their jobs actually have it. This reduces insider abuse and accidental data leakage.
- **Implement controls and monitoring tools to access privileged systems and data:** Stay informed about who accesses what data when and be alerted when suspicious activities occur. Log files and analytics systems provide early warnings of breaches.
- **Protect your mobile and cloud applications:** Improve security with context-based adaptive MFA and eliminate the use of easy-to-remember, reused, and/or improperly stored passwords to secure app access.
- **Stop breaches that start on endpoints:** Grant access to apps and infrastructure only from trusted and secured endpoints. Manage and secure your heterogeneous endpoints through a single source of identity and a least-privilege access model.
- **Implement portals for accessing the web as SaaS applications:** Improve end-user productivity and secure every user's access to apps through federated SSO to eliminate the risk of redirection to phishing websites.

14.5 Intrusion Detection

It is useful to begin by defining the following terms:

- **Intrusion:** Violations of security policy, usually characterized as attempts to affect the confidentiality, integrity, or availability of a computer or network. These violations come from attackers accessing systems from the Internet or from authorized users of the systems attempting to overstep their legitimate authorization levels or using their legitimate access to the system to conduct unauthorized activity.
- **Intrusion detection:** The process of collecting information about events occurring in a computer system or network and analyzing them for signs of intrusions.
- **Intrusion detection system (IDS):** Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding and providing real-time or near-real-time warning of attempts to access system resources in an unauthorized manner.

https://t.me/learningnets

IDSs are classified as follows:

- **Host-based IDS:** Monitors the characteristics of a single host and the events occurring within that host for suspicious activity. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the operating system. Furthermore, unlike network-based IDSs, host-based IDSs more readily see the intended outcome of an attempted attack because they directly access and monitor the data files and system processes usually targeted by attacks.
- **Network-based IDS:** Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

An IDS comprises three logical components:

- **Sensors:** Sensors are responsible for collecting data. The input for a sensor is any part of a system that contains evidence of an intrusion. Types of input to a sensor include network packets, log files, and system call traces. Sensors collect and forward this information to an analyzer.
- **Analyzers:** Analyzers receive input from one or more sensors or from other analyzers. The analysis engines are responsible for determining if an intrusion has occurred. The output of this component may include evidence supporting the conclusion that an intrusion occurred. The analyzer provides guidance about what actions to take as a result of an intrusion.
- **User interface:** The user interface to an IDS enables a user to view output from the system or control the behavior of the system. In some systems, the user interface may equate to a manager, director, or console component.

Basic Principles

Authentication facilities, access control facilities, and firewalls all play roles in countering intrusions. Another line of defense is intrusion detection, and it has been the focus of much research in recent years. This interest has been motivated by several considerations, including the following:

- If an intrusion is detected quickly enough, the intruder is identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not timely enough to preempt the intruder, the sooner the intrusion is detected, the less damage can be done and the more quickly recovery can be achieved.

https://t.me/learningnets

- An effective IDS serves as a deterrent, acting to prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques used to strengthen intrusion prevention measures.

Approaches to Intrusion Detection

Intrusion detection assumes that the behavior of the intruder differs from that of a legitimate user in ways that are quantifiable. Of course, you cannot expect that there will be a crisp, exact distinction between an attack by an intruder and the normal use of resources by an authorized user. Rather, you must expect that there will be some overlap.

There are two general approaches to intrusion detection: misuse detection and anomaly detection (see Figure 14.5).

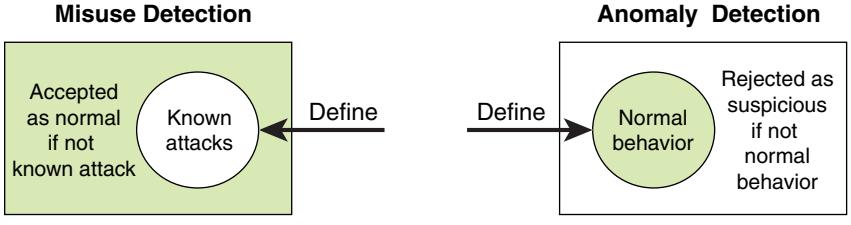


FIGURE 14.5 Approaches to Intrusion Detection

Misuse detection is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents. Misuse detectors use various pattern-matching algorithms, operating on large databases of attack patterns, or *signatures*. An advantage of misuse detection is that it is accurate and generates few false alarms. A disadvantage it that it cannot detect novel or unknown attacks.

Anomaly detection involves searching for activity that is different from the normal behavior of system entities and system resources. An advantage of anomaly detection is that it is able to detect previously unknown attacks based on an audit of activity. A disadvantage is that there is a significant trade-off between false positives and false negatives. Figure 14.6 suggests, in abstract terms, the nature of the task confronting the designer of an anomaly detection system. Although the typical behavior of an intruder differs from the typical behavior of an authorized user, there is some overlap in these behaviors. Thus, a loose interpretation of intruder behavior, which catches more intruders, also leads to a number of *false positives*, or authorized users identified as intruders. On the other hand, an attempt to limit false positives by a tight interpretation of intruder behavior leads to an increase in *false negatives*, or intruders not

https://t.me/learningnets

identified as intruders. Thus, there is an element of compromise and art in the practice of anomaly detection.

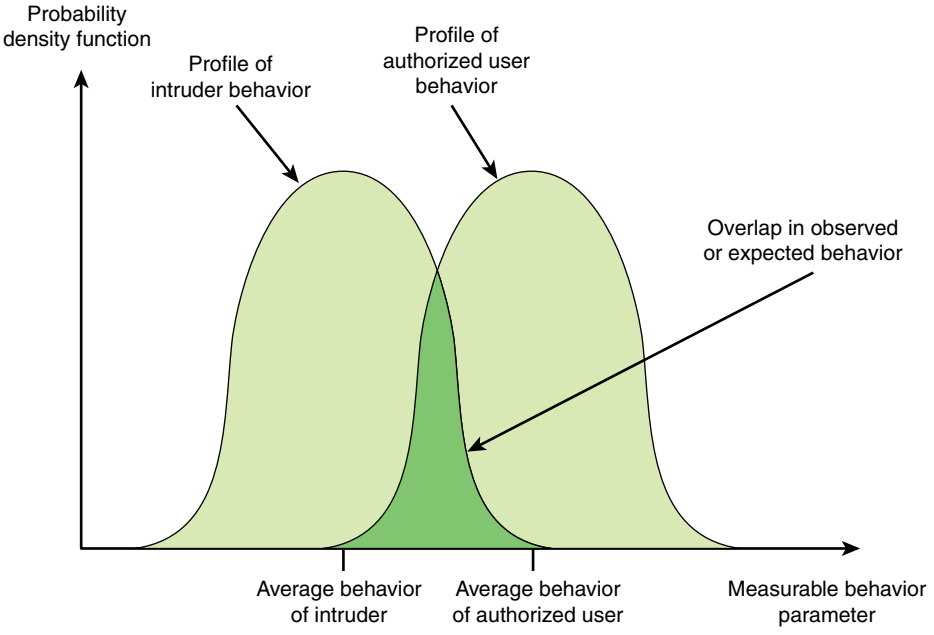


FIGURE 14.6 Profiles of Behavior of Intruders and Authorized Users

Table 14.2 clarifies the relationship between the terms *false positive*, *true positive*, *false negative*, and *true negative*.

TABLE 14.2 Test Outcomes

Test result	Condition A Occurs	Condition A Does Not Occur
Test says "A"	True positive	False positive
Test says "NOT A"	False negative	True negative

Host-Based Intrusion Detection Techniques

Host-based IDSs add a specialized layer of security software to vulnerable or sensitive systems; examples include database servers and administrative systems. A host-based IDS monitors activity on a system in a variety of ways to detect suspicious behavior. In some cases, an IDS halts an attack before any damage is done, but its primary purpose is to detect intrusions, log suspicious events, and send alerts.

The primary benefit of a host-based IDS is that it detects both external and internal intrusions—something that is not possible either with network-based IDSs or firewalls.

https://t.me/learningnets

Host-based IDSs use either anomaly or misuse protection or a combination of the two. For anomaly detection, two common strategies are:

- **Threshold detection:** This approach involves defining thresholds, independent of the user, for the frequency of occurrence of various events.
- **Profile based:** A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

Network-Based Intrusion Detection Systems

A network-based IDS (NIDS) monitors the traffic on the network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments and traffic on other means of communication (such as phone lines) can't be monitored by a single NIDS.

NIDS Function

Network-based intrusion detection involves looking at the packets on a network as they pass by some sensor. Packets are considered to be of interest if they match a signature. Three primary types of signatures are string signatures, port signatures, and header condition signatures.

A string signature looks for a text string that indicates a possible attack. An example of a string signature for UNIX might be **"cat "+ +" > /.rhosts"**, which, if successful, might cause a UNIX system to become extremely vulnerable to network attack. To refine the string signature to reduce the number of false positives, it may be necessary to use a compound string signature. A compound string signature for a common web server attack might be **"cgi-bin" AND "aglimpse" AND "IFS"**.

A port signature watches for connection attempts to well-known, frequently attacked ports. Examples of these ports include those for Telnet (TCP port 23), FTP (TCP port 21/20), SUNRPC (TCP/UDP port 111), and IMAP (TCP port 143). If any of these ports are not used by the site, then incoming packets to these ports are suspicious.

A header signature watches for dangerous or illogical combinations in packet headers. The most famous example is WinNuke, where a packet was destined for a NetBIOS port and the urgent pointer, or out-of-band pointer, was set. This resulted in the "blue screen of death" for Windows systems. Another well-known header signature is a Transmission Control Protocol (TCP) packet with both the synchronize (SYN) and finished (FIN) flags set, signifying that the requestor wishes to start and stop a connection at the same time.

https://t.me/learningnets

NIDS Placement

A NIDS sensor sees only the packets that are carried on the network segment to which it is attached. Accordingly, a NIDS deployment is typically set up as a number of sensors distributed on key network points to passively gather traffic data and feed information on potential threats to a central NIDS manager. Figure 14.7 provides examples of NIDS sensor

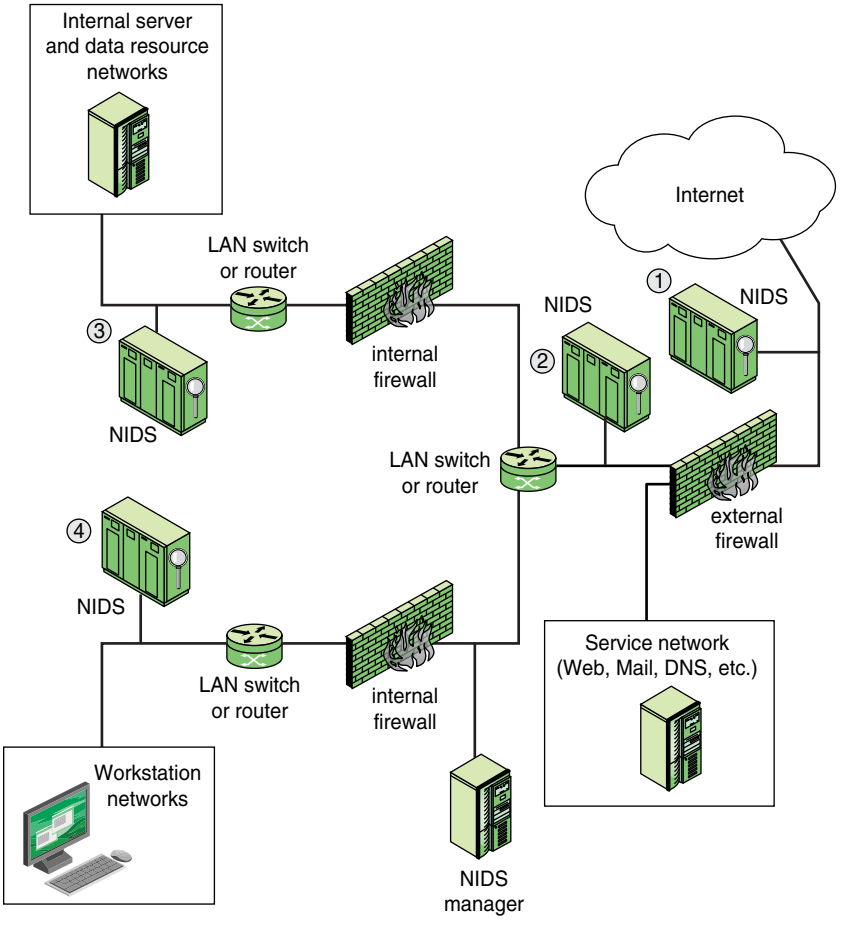


FIGURE 14.7 NIDS Sensor Deployment Example

There are four types of locations for the sensors:

- **Outside the main enterprise firewall:** This placement is useful for establishing the level of threat for a given enterprise network. Those responsible for winning management support for security efforts find this placement valuable.

https://t.me/learningnets

demilitarized zone (DMZ)

A perimeter network segment that is physically or logically between internal and external networks. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than to the entire internal network. This provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

- **In the network demilitarized zone (DMZ), inside the main firewall but outside internal firewalls:** This location monitors for penetration attempts that target web and other services that are generally open to outsiders.
- **Behind internal firewalls:** A sensor can be positioned to monitor major backbone networks, such as those that support internal servers and database resources.
- **Behind internal firewalls:** A sensor can be positioned to monitor LANs that support user workstations and servers specific to single departments. Locations 3 and 4 in Figure 14.7 can monitor for more specific attacks at network segments, as well as attacks originating from inside the organization.

IDS Best Practices

The following are some suggestions that security managers may find helpful:

- Create separate accounts for each IDS user and administrator.
- Restrict network access to IDS components.
- Ensure that IDS management communications are protected appropriately, such as encrypting them or transmitting them over a physically or logically separate network.
- Back-up IDS configuration settings periodically and before applying updates to ensure that existing settings are not inadvertently lost.
- Monitor and tune one IDS sensor at a time to prevent security staff from being overwhelmed by alerts and false positives.
- Have alerts of a certain priority sent directly to a security administrator so attacks are quickly known or when other events might require administration attention. To reduce the noise, set alerts only to the risks the enterprise is most concerned about and don't rely on out-of-the box settings.
- Employ a log and alert correlation product (such as a security information event management [SIEM]system) in conjunction with the IDS. These correlation products do several things. First, they group alerts to reduce alert traffic. Instead, batches of alerts or events arrive in more manageable increments. They also provide insight across multiple platforms, including network and host IDSs, firewalls, and syslog events from other systems.
- Have a system in place to ensure that IDS event logs are reviewed regularly. An example of such a product is Sguil, which is a free set of software packages.



Sguil http://bammv.github.io/sguil/index.html

https://t.me/learningnets

A useful resource is SP 800-94, *Guide to Intrusion Detection and Prevention Systems*, which contains a tutorial on IDS function and a range of recommendations related to the procurement and management of IDSs.

14.6 Data Loss Prevention

Data loss is intentional or unintentional release of information to an untrusted environment. *Data loss prevention* (*DLP*), also referred to as *information leakage*, refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (for example, endpoint actions), data in motion (for example, network actions), and data at rest (for example, data storage) through deep content inspection and with a centralized management framework. Over the past several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network and to securing the data itself. DLP controls are based on policy and include classifying sensitive data, discovering data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance. Sensitive information that is at risk of leakage or is actually leaked often includes shared and unencrypted content such as word processing documents, presentation files, and spreadsheets that could leave an organization via many different points or channels (for example, via email, instant messaging, Internet browsing, mobile devices, or on portable storage devices).

Data Classification and Identification

All sensitive data within an enterprise needs to be protected at all times and in all places. As a first step, an enterprise needs to define what is sensitive data and, if necessary, establish different levels of sensitive data. Then there is a need to recognize sensitive data wherever it is encountered in the enterprise. Finally, there must be applications that recognize sensitive data in real time. The following are common approaches to the recognition task [MOGU07]:

- **Rule-based recognition:** Regular expressions, keywords, and other basic pattern-matching techniques are best suited for basic structured data, such as credit card and Social Security numbers. This technique efficiently identifies data blocks, files, database records, and so on that contain easily recognized sensitive data.
- **Database fingerprinting:** This technique searches for exact matches to data loaded from a database, which can include multiple field combinations, such as name, credit card number, and CVV number. For example, a search could look only for credit card numbers in the customer base, thus ignoring employees buying online. This is a time-consuming technique but has a very low false positive rate.

https://t.me/learningnets

hash value
A numeric value produced by a mathematical function that generates a fixed-length value typically much smaller than the input to the function. The function is many-to-one, but generally, each file or other data block input to a hash function yields a unique hash value.

- **Exact file matching:** This technique involves computing the **hash value** of a file and monitoring for any files that match the exact fingerprint. It is easy to implement and checks whether a file has been accidentally stored or transmitted in an unauthorized manner. However, unless a more time-consuming cryptographic hash function is used, this is trivial for an attacker to evade.
- **Partial document matching:** This technique involves looking for a partial match on a protected document. It involves the use of multiple hashes on portions of the document, such that if a portion of the document is extracted and filed elsewhere or pasted into an email, it can be detected. This technique is useful for protecting sensitive documents.

Data States

Key to effective DLP is to develop an understanding of the places and times at which data are vulnerable. A useful way of managing DLP is to categorize data into three states: data in motion, data at rest, and data in use. Corresponding to these three states are three key DLP objectives:

- **Data at rest:** Locate and catalog sensitive information stored throughout the enterprise.
- **Data in motion (or transit):** Monitor and control the movement of sensitive information across enterprise networks.
- **Data in use:** Monitor and control the movement of sensitive information on end-user systems.

Data at Rest

Data at rest presents significant risk for enterprises. A large enterprise may have millions of files and database records on drives and removable media. A particular set of data files or records may have a "home" location, but portions of that data may also migrate to other storage locations, and this situation, if not monitored and controlled, quickly becomes unmanageable. One example of how data is replicated and proliferated is file sharing. With networked computer systems, file sharing for collaborative projects is common, but this may mean that the owner or creator of a file has no idea of what happened to the file after sharing it. The same risk exists with the many web-based collaboration and document management platforms in common use.

The fundamental task of DLP for data at rest is to identify and log where specific types of information are stored throughout the enterprise. The DLP unit uses some sort of data discovery agent that performs actions, as shown in Figure 14.8.

https://t.me/learningnets

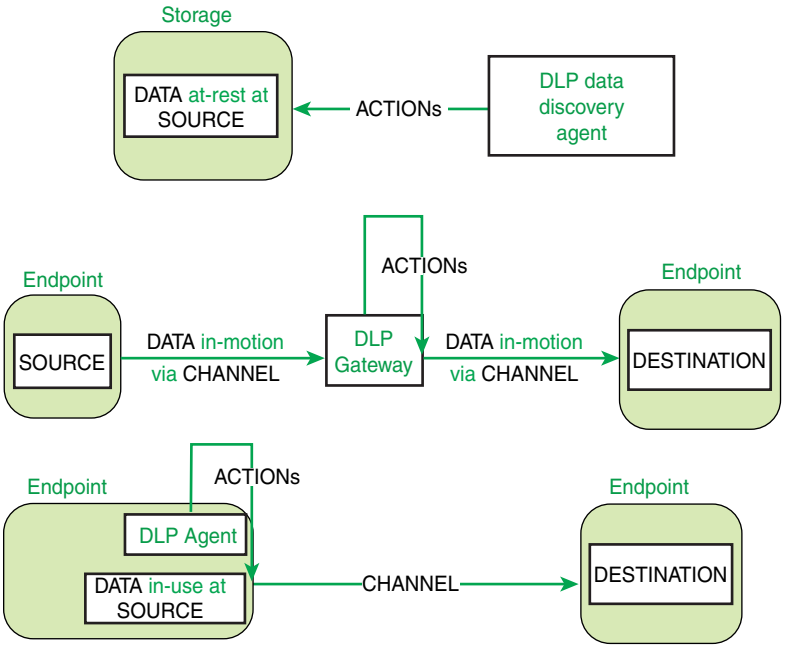


FIGURE 14.8 DLP Models

These actions are as follows:

- Seek out and identify specific file types, such as spreadsheets, word processing documents, email files, and database records. The search activity encompasses files servers, storage area networks, network attached storage, and endpoint systems.
- Once files are found, the agent must be able to open each file to scan the content for specific types of information.
- The agent logs files that contain information of security relevance, and may issue alerts if a security policy is violated.

Data in Motion

The term *data in motion* refers to data transmitted over enterprise networks and between the enterprise networks and external network links. Data-in-motion solutions operate in one of two modes:

- **Passive monitoring:** Observes a copy of data packets as they move across a network link. This is done by a **port mirror** on a switch or a network line tap.

port mirror
A cross-connection of two or more ports on a network switch so that traffic is simultaneously sent to a network analyzer or monitor connected to another port.

https://t.me/learningnets

Packets or sequences of packets containing information of interest are logged, and security violations trigger an alert.

- **Active monitoring:** Interposes a relay or gateway type of device on a network line to analyze and forward data packets (refer to Figure 14.8). The active monitor logs and issues alerts but can also be configured to block data flows that violate a security policy.

To inspect the information being sent across the network, the DLP solution must be able to monitor the network traffic, recognize the correct data streams to capture, assemble the collected packets, reconstruct the files carried in the data stream, and then perform the same analysis that is done on the data at rest to determine whether any portion of the file contents is restricted by its rule set.

Data in Use

Data-in-use solutions generally involve installing DLP agent software on endpoint systems. The agent monitors, reports, blocks, or quarantines the use of particular kinds of data files and/or the contents of a file. The agent also maintains an inventory of files on the hard drives and removable media that is plugged in to the endpoint. The agent either allows or disallows certain types of removable media, such as requiring that the removable device support encryption.

14.7 Digital Rights Management

Digital rights management (DRM) refers to systems and procedures which ensure that holders of digital rights are clearly identified and receive the stipulated payment for their works. The systems and procedures can also impose further restrictions on the use of digital objects, such as inhibiting printing or prohibiting further distribution.

There is no single DRM standard or architecture. DRM encompasses a variety of approaches to intellectual property management and enforcement by providing secure and trusted automated services to control the distribution and use of content. In general, the objective is to provide mechanisms for the complete content management life cycle (creation, subsequent contribution by others, access, distribution, use), including the management of rights information associated with the content.

DRM systems should meet the following objectives:

- Provide persistent content protection against unauthorized access to the digital content, limiting access to only those with the proper authorization.
- Support a variety of digital content types (for example, music files, video streams, digital books, images).

https://t.me/learningnets

- Provision content use on a variety of platforms (for example, PCs, tablets, mobile phones).
- Facilitate content distribution on a variety of media (for example, CD-ROMs, DVDs, flash memory).

DRM Structure and Components

DRM is best understood in terms of the key components of a DRM system and their interconnections. Figure 14.9 illustrates a typical DRM model in terms of the principal users of DRM systems.

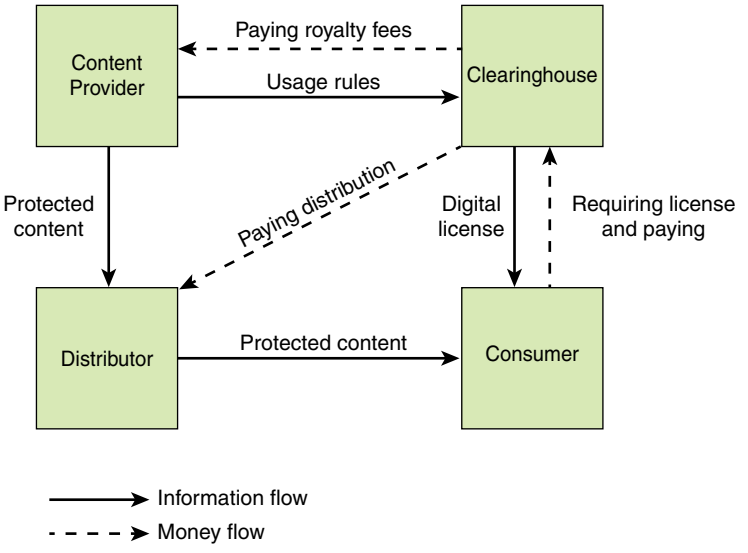


FIGURE 14.9 DRM Components

The principal users of DRM systems are as follows:

- **Content provider:** Holds the digital rights to the content and wants to protect these rights. Examples are a music record label and a movie studio.
- **Distributor:** Provides distribution channels, such as an online shop or a web retailer. For example, an online distributor receives the digital content from the content provider and creates a web catalog presenting the content and rights metadata for the content promotion.
- **Consumer:** Uses the system to access the digital content by retrieving downloadable or streaming content through the distribution channel and then paying

https://t.me/learningnets

for the digital license. The player/viewer application used by the consumer takes charge of initiating license request to the clearinghouse and enforcing the content usage rights.

- **Clearinghouse:** Handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly. The clearinghouse is also responsible for logging license consumptions for the individual consumers.

In this model, the distributor need not enforce the access rights. Instead, the content provider can protect the content in such a way (typically encryption) that the consumer must purchase a digital license and access capability from the clearinghouse. The clearinghouse consults usage rules provided by the content provider to determine what access is permitted and the fee for a particular type of access. Having collected the fee, the clearinghouse credits the content provider and distributor appropriately.

Figure 14.10 shows a generic system architecture that supports DRM functionality. The system is access by parties in three roles. *Rights holders* are the content providers, who either created the content or have acquired rights to the content. *Service providers* include distributors and clearinghouses. *Consumers* are those who purchase the right to access to content for specific uses.

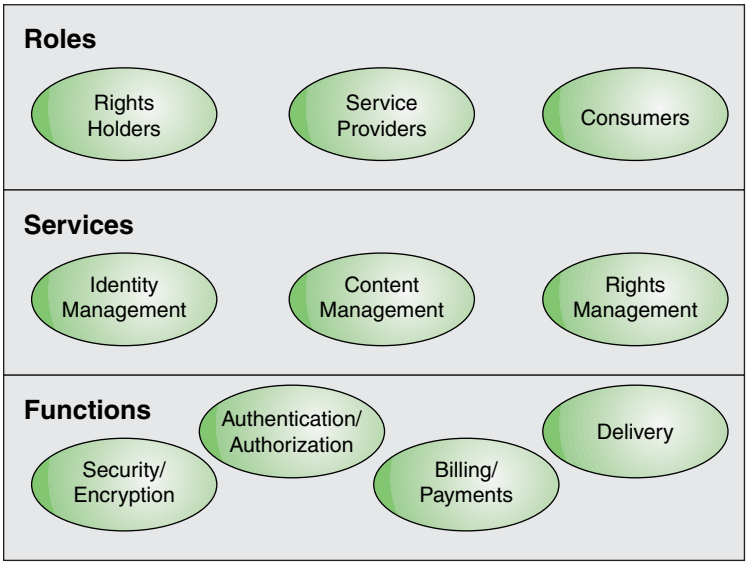


FIGURE 14.10 DRM System Architecture

https://t.me/learningnets

The following services are provided by a DRM system:

- **Identity management:** Mechanisms to uniquely identify entities, such as parties and content
- **Content management:** Processes and functions needed to manage the content lifestyle
- **Rights management:** Processes and functions needed to manage rights, rights holders, and associated requirements

Each management module is a set of common functions. The security/encryption module provides functions to encrypt content and to sign license agreements. The identity management service makes use of the *authentication* and *authorization* functions to identify all parties in the relationship. Using these functions, the identity management service includes the following:

- Allocation of unique party identifiers
- User profiles and preferences
- User device management
- Public key management

Billing/payments functions deal with the collection of usage fees from consumers and the distribution of payments to rights holders and distributors. Delivery functions deal with the delivery of content to consumers.

DRM Best Practices

A report from NSS Labs [BAYL13] lists the following DRM best practices:

- Create a document classification matrix prior to implementing the solution. This matrix should classify data types according to risk and is usually composed of either three or five classifications, with public data having a score of 1, and highly classified material having the highest rating. Each data classification should include mandatory controls that cover data protection while at rest and when in motion, with more sensitive data requiring rigorous access and audit logs. Integrate this classification matrix with existing authentication systems, such as password, MFA, or SSO. This ensures that only active accounts are able to access sensitive documents and also provides an audit trail from an official system of record (SOR).

https://t.me/learningnets

- Begin user education to obtain employee buy-in. This is critical to ensure protection of existing data and of newly created data. A risk-based approach is favored here, where those with regular access to confidential data should be thoroughly trained in their responsibilities. Users must understand the risk of data loss and the repercussions to their organization as a result of this data loss. Data owners must be responsible for appropriate labeling and protection of their data, and they should be familiarized with the relevant management-endorsed policies. Before deploying DLP or DRM systems, enterprises should attempt to manage contractor, partner, and/or employee use of public cloud systems (for example, Dropbox, iCloud) for storage of corporate data.
- Recognize where the existing data resides and how those data are classified. Interview executives and peers to understand data flows within and outside the network. Examine controls and data stores currently in place. Seek out unprotected copies of confidential data; this data should be protected or deleted. Focus on first protecting the most sensitive category of data. In large enterprises, it is advisable to start with the highest-risk documents that are most likely to be exposed to greater risk (for example, be sent to an outside entity that is not fully trusted). Only when the most sensitive category of data has been protected throughout the enterprise is it safe to move to the next tier.
- Identify top data loss scenarios. Knowledge of where data is, what form it takes, and who has access to this data will enable creation of tailored controls. These controls reduce the risk of data loss and lessen the damage resulting from such data loss scenarios. This measure requires a thorough understanding of business needs and practices, regulatory requirements, risk, and likely repercussions of data loss. Be sure to clearly define the classes of violation and specify real repercussions for offenders. Have documentation from HR, legal personnel, and senior management that supports the stipulation that rule violations will result in appropriate penalties. Users working with highly sensitive data must ensure that all confidential work is protected by DRM, even when documents are in draft stage.
- Ensure that data owners and IT can easily monitor sensitive file usage; this monitoring of usage will increase knowledge of data usage within the organization. DRM tools should also be leveraged to gain visibility into data flowing across internal networks and to the Internet.
- Strive to make the DRM system user-friendly. Requiring license verification each time a document is opened is good practice for high-security documents

https://t.me/learningnets

or for documents that need to be revoked instantly. However, be aware that requiring license checks creates access issues because these documents can never be used offline. There is an element of risk in that a previously unauthorized user is able to access the documents during this window of time. Time windows should be configured according to a document's sensitivity and the organization's appetite for risk.

- Review logs and alerts regularly and address suspicious events. Modern DRM solutions enable control of documents even after they have been sent outside the enterprise or downloaded to a recipient's end device. Document control enables users to specify granular control, which includes enabling or restricting recipients from viewing, printing, and copying content. Document permissions are dynamic (the document calls home to obtain updated permissions), and can be modified by the DRM administrator or document owner at any time. Document tracking enables users to follow documents after they have been sent. A full audit log details who opened a document, when, where, and on which device. Some solutions provide a geographic display that shows exactly where a document is being opened. This feature helps prompt investigation if, for example, a sensitive document being accessed by a user at HQ is simultaneously being accessed using the same credentials at a different geographic location.
- Regularly carry out gap analysis that details the differential between the organization's current risk level for data loss and the organization's acceptable risk level. In DRM, it is often difficult to decide if there is an appropriate balance between protecting sensitive documents and keeping the permissions appropriate. If additional rules, policies, training, procedures, or technologies are warranted, these can be implemented, once they are endorsed by executive stakeholders.

14.8 Cryptographic Solutions

This section and the next two sections look at important aspects of the use of cryptography. Brief technical introductions are provided in each section. For a more detailed treatment, see *Cryptography and Network Security* by Stallings [STAL17].

Uses of Cryptography

Cryptography is used to protect data at rest and data in motion, both inside and outside the boundaries of an enterprise's IT system. Within a system, logical and physical

https://t.me/learningnets

access control, intrusion detection, firewall, and other security controls—possibly supplemented by cryptography—provide sufficient protection. But outside the control of the enterprise, using cryptography is often the only way to protect data. Four uses for cryptography predominate:

- **Data encryption:** Data encryption is a powerful and cost-effective means of providing data confidentiality and integrity. Once data are encrypted, the ciphertext does not have to be protected against disclosure. Further, if ciphertext is modified, it does not decrypt correctly. Data encryption is especially useful for transmitting data over the Internet or other network outside the control of the enterprise and also for storage in the cloud.
- **Data integrity:** Cryptographic algorithms provide an effective way to determine whether a block of data (for example, email text, message, file, database record) was altered in an unauthorized manner.
- **Digital signature:** The digital signature, or electronic signature, is the electronic equivalent of a written signature that is recognized as having the same legal status as a written signature. In addition to ensuring data integrity, digital signature algorithms provide a means of linking a document with a particular entity, as is done with a written signature.
- **User authentication:** Cryptography is the basis for several advanced authentication methods. Instead of communicating passwords over an open network, authentication involves demonstrating knowledge of a cryptographic key. Using such a method, a one-time password that is not susceptible to eavesdropping is used.

cryptographic algorithm

An algorithm that uses the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key-agreement algorithms.

Cryptographic Algorithms

Cryptographic algorithms fall into three broad categories: encryption/decryption algorithms, secure hash algorithms, and digital signature algorithms. Let's examine each in turn.

Symmetric Encryption

Symmetric encryption, also referred to as *conventional encryption*, is a cryptographic scheme in which encryption and decryption are performed using the same key. A symmetric encryption scheme has five ingredients, as shown in Figure 14.11a:

https://t.me/learningnets

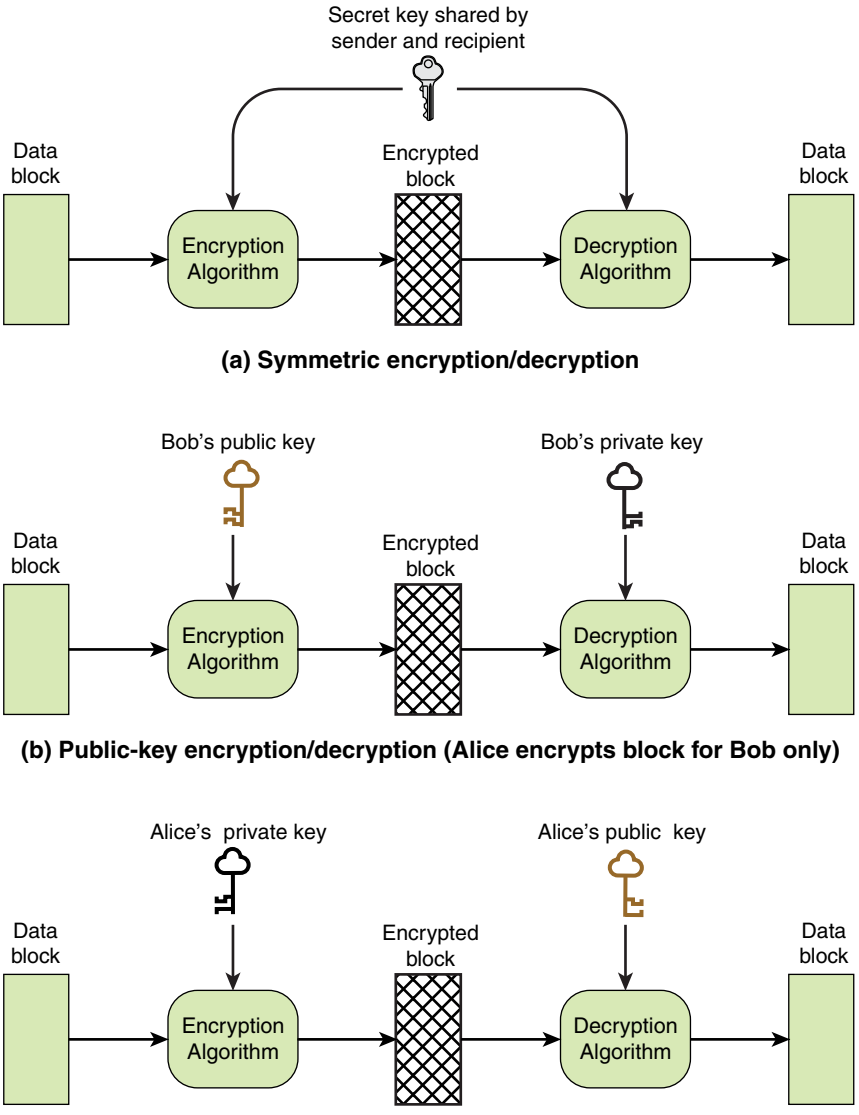


FIGURE 14.11 Symmetric and Public Key Encryption

- **Plaintext:** This is the original message or data block that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

https://t.me/learningnets

- **Secret key:** The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given data block, two different keys will produce two different ciphertexts.
- **Decryption algorithm:** This is the inverse of the encryption algorithm. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of symmetric encryption:

- You need a strong encryption algorithm. At a minimum, the algorithm should be such that an opponent who knows the algorithm and has access to one or more ciphertexts is unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
- The sender and receiver must obtain copies of the secret key in a secure fashion and keep the key secure. If someone discovers the key and knows the algorithm, all communication using this key is readable.

There are two general approaches to attacking a symmetric encryption scheme. The first attack is known as *cryptanalysis*. Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext/ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised. The second method, known as a *brute-force attack*, is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success. Thus a secure symmetric encryption scheme requires a secure algorithm and a key of sufficient length to defeat a brute-force attack.

Public Key Encryption

Public key cryptography, also called *asymmetric cryptography*, involves the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication. A public key encryption scheme has several ingredients:

https://t.me/learningnets

- **Plaintext:** This is the readable message or data block that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.
- **Public key and private key:** This is a pair of keys that were selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input.
- **Ciphertext:** This is the scrambled block produced as output. It depends on the plaintext and the key. For a given message, two different keys produce two different ciphertexts.
- **Decryption algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

The process works (that is, produces the correct plaintext on output) regardless of the order in which the pair of keys is used. As the names suggest, the public key of the pair is made public for others to use, while the private key is known only to its owner.

Suppose that Alice wants to send a private message to Bob. Also suppose that she has Bob's public key, and Bob has the matching private key (Figure 14.11b). Using Bob's public key, Alice encrypts the message to produce ciphertext. The ciphertext is then transmitted to Bob. When Bob gets the ciphertext, he decrypts it using his private key. Because only Bob has a copy of his private key, no one else can read the message.

Public key encryption can be used in another way, as illustrated in Figure 14.11c. Suppose that Alice wants to send a message to Bob and, although it isn't important that the message be kept secret, she wants Bob to be certain that the message is indeed from her. In this case, Alice uses her own private key to encrypt the message. When Bob receives the ciphertext, he finds that he can decrypt it with Alice's public key, thus proving that the message must have been encrypted by Alice: No one else has Alice's private key, and therefore no one else could have created a ciphertext that could be decrypted with Alice's public key.

As with symmetric encryption algorithms, the security of public key encryption depends on the strength of the algorithm and the length of the private key. Public key cryptographic algorithms are considerably slower than symmetric algorithms for a given data block length. Accordingly, public key cryptographic is almost always limited to use with small blocks of data, such as a secret key or, as discussed next, a hash value.

https://t.me/learningnets

Secure Hash Functions

As with any hash function, a secure hash function takes a variable-length block of data as input and produces a fixed-length hash value that is typically shorter than the input data block. Secure hash functions are an essential element of many security protocols and applications. To be useful for security applications, a hash function H must have the properties indicated in Table 14.3.

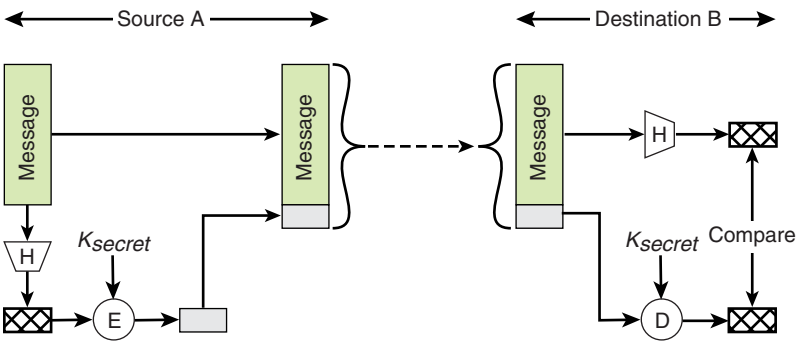
TABLE 14.3 Requirements for a Cryptographic Hash Function H

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).
Pseudorandomness	Output of H meets standard tests for pseudorandomness.

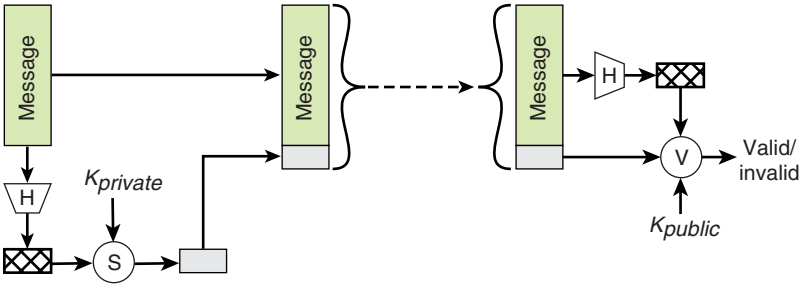
Figure 14.12 indicates two common ways in which hash functions are used. Figure 14.12a illustrates the use of a hash function to ensure the data integrity of a block of data, generally referred to as *message authentication*. The two important aspects of message authentication are to verify that the content of the message was not altered and to verify that the source is authentic. You can also verify a message's timeliness (that is, ensure that it has not been artificially delayed and replayed) and that the sequence is relative to other messages flowing between two parties.

For message authentication, a hash value is generated for the source message. The hash value is then encrypted using a secret key shared by a cooperating partner. Then the message and the encrypted hash value are transmitted to the destination. The recipient decrypts the incoming encrypted hash value, generates a new hash value from the incoming message, and compares the two hash values. If you assume that

https://t.me/learningnets



(a) Message authentication using symmetric encryption



(b) Digital signature using public-key encryption

E = encryption algorithm
D = decryption algorithm
H = hash function
S = signing algorithm
V = verifying algorithm

FIGURE 14.12 Uses for Secure Hash Functions

only the receiver and the sender know the identity of the secret key, and if the received code matches the calculated code, then the following occurs:

1. The receiver is assured that the message was not altered. If an attacker alters the message but does not alter the code, then the receiver's calculation of the code differs from the received code. For a secure hash function, it is infeasible for an attacker to alter the message in such a way that the hash value is not altered.
2. The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper code.
3. If the message includes a sequence number (such as is used with High-Level Data Link Control [HDLC] and TCP), then the receiver is assured of the proper sequence because an attacker cannot successfully alter the sequence number.

https://t.me/learningnets

A second important use for hash functions is in the digital signature process, explained next.

Digital Signatures

NIST FIPS 86-3, *Digital Signature Standard*, defines *digital signature* as follows:

> The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.

Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block. Another agent can access the data block and its associated signature and verify that (1) the data block was signed by the alleged signer and that (2) the data block was not altered since the signing. Further, the signer cannot repudiate the signature.

Figure 14.12b illustrates the digital signature process. Suppose that Bob wants to sign a document or message. Although it is not important that the message be kept secret, he wants others to be certain that the message is indeed from him. For this purpose, Bob uses a secure hash function to generate a hash value for the message. That hash value and Bob's private key serve as input to a digital signature generation algorithm that produces a short block which functions as a digital signature. Bob sends the message with the signature attached. Any other user can calculate a hash value for the message. The user then inputs that hash value, the attached signature, and Bob's public key to a digital signature verification algorithm. If the algorithm returns the result that the signature is valid, the user is assured that the message must have been signed by Bob. No one else has Bob's private key, and therefore no one else can create a signature to verify this message with Bob's public key. In addition, it is impossible to alter the message without access to Bob's private key, so the message is authenticated both in terms of source and in terms of data integrity. The message also has the feature of nonrepudiation. Bob cannot deny signing the message because no one else could have done so.

Digital signatures are widely used for a number of purposes, including the following:

- Digitally signing email messages to authenticate the sender
- Digitally signing a software program to authenticate the source of the program and to counter the threat of software tampering
- Verifying the authorship or origin of digital data

https://t.me/learningnets

- Ensuring the integrity of digital data against tampering
- Authenticating online entities

Selection of Cryptographic Algorithms and Lengths

As processor speeds and capacity have increased, and as cryptographic algorithms have been subjected to increased scrutiny, algorithms that were once considered secure have been abandoned. Similarly, key lengths and hash value lengths once considered secure are now too weak for secure use. Accordingly, security managers should take care to choose algorithms and lengths to achieve the desired level of security. A useful source of guidance on algorithm selection is FIPS-140-2A, *Approved Security Functions for FIPS PUB 140-2*, and a useful guide for key and hash length is SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. The ENISA report *Algorithms, Key Size and Parameters—2014* [ENIS14] offers similar recommendations.

For symmetric encryption, NIST recommends the use of Advanced Encryption Standard (AES), with a key length of 128, 192, or 256 bits. AES is widely accepted worldwide and has become the standard symmetric encryption algorithm.

For the hash function, NIST recommends one of two NIST standard hash functions, SHA-2 or SHA-3. The approved hash lengths for these two functions range from 224 to 512 bits. The structure and functions used for SHA-3 are substantially different from those shared by SHA-2 and SHA-1. Thus, if weaknesses are discovered in either SHA-2 or SHA-3, users have the option of switching to the other standard. SHA-2 has held up well, and NIST considers it secure for general use. So for now SHA-3 is a complement to SHA-2 rather than a replacement. The relatively compact nature of SHA-3 makes it useful for "embedded," or smart, devices that connect to electronic networks but that are not themselves full-fledged computers. Examples include sensors in a building-wide security system and home appliances that are controlled remotely.

For digital signatures, NIST recommends three alternative digital signature algorithms:

- Digital Signature Algorithm (DSA) with length of 2,048 bits
- Rivest–Shamir–Adleman (RSA) algorithm with 2,048 bits
- Elliptic-Curve Digital Signature Algorithm with length of 224 bits

https://t.me/learningnets

Cryptography Implementation Considerations

SP 800-12, *An Introduction to Information Security*, lists the following as important management considerations for implementing cryptography within an organization:

- **Selecting design and implementation standards:** It is almost always advisable not to rely on a proprietary cryptographic algorithm, especially if the algorithm itself is secret. Standardized algorithms, such as AES, Secure Hash Algorithm (SHA), and DSA are subject to intense scrutiny by the professional community, and managers can have a high degree of confidence that the algorithms themselves, with the recommended lengths, are secure. NIST and other organizations have developed numerous standards for designing, implementing, and using cryptography and for integrating it into automated systems. Managers and users of systems should choose the appropriate cryptographic standard based on a cost-effectiveness analysis, trends in the standard's acceptance, and interoperability requirements.
- **Deciding between hardware, software, and firmware implementations:** The trade-offs among security, cost, simplicity, efficiency, and ease of implementation need to be studied by managers acquiring various security products meeting a standard.
- **Managing keys:** This topic is addressed in Section 14.9.
- **Ensuring security of cryptographic modules:** A cryptographic module contains the cryptographic algorithm(s), certain control parameters, and temporary storage facilities for the key(s) being used by the algorithm(s). The proper functioning of cryptography requires the secure design, implementation, and use of the cryptographic module. This includes protecting the module against tampering. A useful tool is the NIST Cryptographic Module Validation Program (CMVP), which validates vendor offerings using independent accredited laboratories. The validation is against the security requirements in FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 104-2 provides a detailed set of requirements at four security levels against which vendor hardware, firmware, and software offerings are evaluated (see Table 14.4).



NIST Cryptographic Module Validation Program https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program

- **Applying cryptography to networks:** The use of cryptography in networking applications often requires special considerations. In these applications, the suitability of a cryptographic module depends on its capability for handling special requirements imposed by locally attached communications equipment or imposed by the network protocols and software.

https://t.me/learningnets

TABLE 14.4 Cryptographic Module Security Requirements from FIPS 140-2

Design and Implementation Areas	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic module specification	Specification of cryptographic module, cryptographic boundary, approved algorithms, and approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic module ports and interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, services, and authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite state model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical security	Production-grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. Environmental failure protection (EFP) or environmental failure testing (EFT).
Operational environment	Single operator. Executable code. Approved integrity technique.	Referenced protection profiles (PPs) evaluated at EAL2 (Evaluation Assurance Level 2) with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.

https://t.me/learningnets

Design and Implementation Areas	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic key management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 Code of Federal Regulations (CFR) Federal Communications Commission (FCC) Part 15. Subpart B, Class A (business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (home use).	
Self-tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of other attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

CFR = Code of Federal Regulations

EAL = evaluation assurance level

EMI/EMC = electromagnetic interference/electromagnetic compatibility

PP = protection profile

cryptosystem (cryptographic system)

A set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context.

14.9 Cryptographic Key Management

Key management is the process of administering or managing cryptographic keys for a **cryptosystem (cryptographic system)**. It involves the generation, creation, protection, storage, exchange, replacement, and use of keys and enables selective restriction for certain keys. In addition to access restriction, key management also involves the monitoring and recording of each key's access, use, and context. A key management system also includes key servers, user procedures, and protocols,

https://t.me/learningnets

including cryptographic protocol design. The security of a cryptosystem is dependent on successful key management.

Cryptographic key management is a complex undertaking. The applications, protocols, and security functions in an organization require the use of many cryptographic keys. There are a number of different types of keys. For each key type, there are issues related to how long the keys should be in use and how to safely store and distribute them. A broad range of management and technical issues must be addressed. Fortunately, solid guidance is available from standards organizations.

NIST has produced a number of useful publications for key management, including:

- **SP 800-57, *Recommendation for Key Management—Part 1: General*:** Provides an overview of key management and general guidance and best practices for the management of cryptographic keying material.
- **SP 800-57, *Recommendation for Key Management—Part 2: Best Practices for Key Management Organization*:** Provides guidance on policy and security planning requirements.
- **SP 800-57, *Recommendation for Key Management—Part 3: Application-Specific Key Management Guidance*:** Provides guidance on using the cryptographic features of current systems.
- **SP 800-130, *Framework for Designing Cryptographic Key Management Systems (CKMS)*:** Contains topics that should be considered by a CKMS designer when developing a CKMS design specification.
- **IR 7956, *Cryptographic Key Management Issues and Challenges in Cloud Services*:** Discusses the key management issues related to the distributed control of keys between an enterprise and a cloud service provider.

ISO published the 11770 set of detailed technical documents on key management:

- **ISO 11770-1, *Key Management—Part 1: Framework*:** Defines a general model of key management that is independent of the use of any particular cryptographic algorithm.
- **ISO 11770-2, *Key Management—Part 2: Mechanisms Using Symmetric Techniques*:** Addresses three different environments for the establishment of shared secret keys: point-to-point key establishment schemes, mechanisms using a key distribution center (KDC), and techniques that use a key translation center (KTC).

https://t.me/learningnets

- **ISO 11770-3, *Key Management—Part 3: Mechanisms Using Asymmetric Techniques*:** Defines key management mechanisms based on asymmetric cryptographic techniques. It specifically addresses the use of asymmetric techniques to achieve the following goals:
  - Establish a shared secret key for use in a symmetric cryptographic technique between two entities *A* and *B* by key agreement. In a secret key agreement mechanism, the secret key is computed as the result of a data exchange between the two entities *A* and *B*. Neither of them should be able to predetermine the value of the shared secret key.
  - Establish a shared secret key for use in a symmetric cryptographic technique between two entities *A* and *B* via key transport. In a secret key transport mechanism, the secret key is chosen by one entity *A* and is transferred to another entity *B*, suitably protected by asymmetric techniques.
  - Make an entity's public key available to other entities via key transport. In a public key transport mechanism, the public key of entity *A* shall be transferred to other entities in an authenticated way, but not requiring secrecy.
- **ISO 11770-4, *Key Management—Part 4: Mechanisms Based on Weak Secrets*:** Defines key establishment mechanisms based on weak secrets—that is secrets that can be readily memorized by a human, and hence, secrets that will be chosen from a relatively small set of possibilities.
- **ISO 11770-5, *Key Management—Part 5: Group Key Management*:** Specifies key establishment mechanisms for multiple entities to provide procedures for handling cryptographic keying material used in symmetric or asymmetric cryptographic algorithms according to the security policy in force.
- **ISO 11770-6, *Key Management—Part 6: Key Derivation***: Specifies key derivation functions—that is, functions that take secret information and other (public) parameters as input and output one or more derived secret keys. Key derivation functions based on MAC algorithms and on hash functions are specified.

group key

A symmetric cryptographic key shared among multiple participants. A block of data encrypted by any one participant using the group key can be decrypted by any other participant who shares the group key.

Key Types

One of the aspects of key management that makes this discipline so complex is the wide variety of key types employed in a cybersecurity deployment. SP 800-57 identifies several different key types:

- **Private and public signature keys:** The asymmetric key pair used to generate and verify digital signatures.

https://t.me/learningnets

- **Symmetric authentication key:** Used for message authentication, as illustrated in Figure 14.12a.
- **Private and public authentication keys:** Used to provide assurance of the identity of an originating entity (that is, source authentication) when establishing an authenticated communication session.
- **Symmetric data encryption key:** Used to provide data confidentiality by encryption/decryption.
- **Symmetric key-wrapping key:** Also called a key-encryption key, is used to encrypt/decrypt other keys.
- **Symmetric random number generation key:** Used with a random number generation algorithm.
- **Symmetric master key:** Used to derive other symmetric keys (for example, data-encryption keys, key-wrapping keys) using symmetric cryptographic methods. The master key is also known as a key-derivation key.
- **Private and public key-transport keys:** Used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Symmetric key-agreement key:** Used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors) using a symmetric key-agreement algorithm.
- **Private and public static key-agreement key:** Long-term key pair used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Private and public ephemeral key-agreement key:** Short-term key pair used only once to establish one or more keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Symmetric authorization key:** Used to provide privileges to an entity. The authorization key is known by the entity responsible for monitoring and granting access privileges for authorized entities and by the entity seeking access to resources.
- **Private and public authorization key:** Used to provide and verify privileges.

https://t.me/learningnets

Cryptoperiod

The cryptoperiod of a cryptographic key is the time span during which a specific cryptographic key is authorized for use for its defined purpose. This is an important consideration. A number of potential security threats make it advisable that any key not be used for a prolonged period of time. These threats include:

- **Brute-force attacks:** As raw processing power and the ability to use numerous processors in parallel increase, a given key length becomes increasingly vulnerable, and longer key lengths are advised. Any of the shorter keys in use need to be retired as quickly as possible and longer key lengths employed. For example, NIST used to recommend the use of 1,024-bit keys for certain asymmetric algorithms but now recommends 2,048 bits for these algorithms.
- **Cryptanalysis:** Over time, flaws may be discovered in a cryptographic algorithm that make it feasible to "break" the algorithm. An example of this is the original NIST standard hash algorithm, SHA-1, which was used in its DSA. Once these weaknesses were discovered, NIST migrated to SHA-2 and SHA-3. Similarly, methods were found for breaking algorithms such as the RSA asymmetric algorithm at rates faster than brute force, which are thwarted by using longer keys.
- **Other security threats:** Beyond simply attacking an algorithm directly in an attempt to discover a key that is being used, there are a variety of other methods of attack. They include attacks on the mechanisms and protocols associated with the keys, key modification, and achieving unauthorized disclosure. The longer a particular key is used for encryption and decryption, the greater the chance that some means of learning the key will succeed.

Accordingly, an enterprise should have policies for the maximum cryptoperiod of each key type.

Figure 14.13 illustrates the two aspects of a cryptoperiod. The originator usage period (OUP) refers to the time during which data is encrypted, and the recipient usage period (RUP) is the time during which such data continues to be maintained in its encrypted form and subject to decryption. The RUP often starts at the beginning of the OUP, but there may be some delay before data is decrypted. More significantly, the end of the RUP may extend a considerable length of time beyond the end of the OUP. That is, the policy may state that a given key may no longer be used for encrypting new data, but the data that has already been encrypted may be retained in the encrypted form, available for decryption for a further period of time. Hence the cryptoperiod extends from the start of the OUP to the end of the RUP.

https://t.me/learningnets

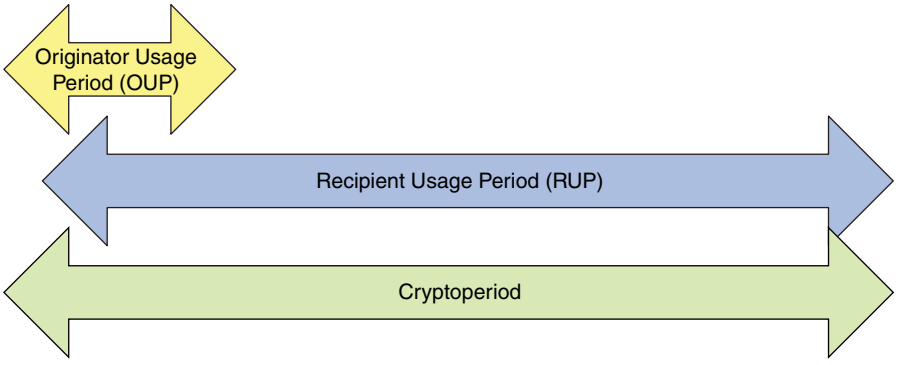


FIGURE 14.13 Cryptoperiod

Table 14.5 shows the cryptoperiods suggested in SP 80-57.

TABLE 14.5 Suggested Cryptoperiods from SP 800-57

Key Type	OUP	RUP
Private signature key	1 to 3 years	—
Public signature-verification key	Several years (depends on key size)	
Symmetric authentication key	≤2 years	≤OUP + 3 years
Private authentication key	1 to 2 years	
Public authentication key	1 to 2 years	
Symmetric data encryption keys	≤2 years	≤OUP + 3 years
Symmetric key-wrapping key	≤2 years	≤OUP + 3 years
Symmetric RBG keys	See SP 800-90	—
Symmetric master key	About 1 year	—
Private key transport key	≤2 years	
Public key transport key	1 to 2 years	
Symmetric key agreement key	1 to 2 years	
Private static key agreement key	1 to 2 years	
Public static key agreement key	1 to 2 years	
Private ephemeral key agreement key	One key-agreement transaction	
Public ephemeral key agreement key	One key-agreement transaction	
Symmetric authentication key	≤2 years	
Private authentication key	≤2 years	
Public authentication key	≤2 years	

https://t.me/learningnets

Key Life Cycle

A key may pass through a number of states between its generation and destruction. Figure 14.14, based on a figure in *Key Management for Dummies* [MOUL11], show the typical life cycle of a key.

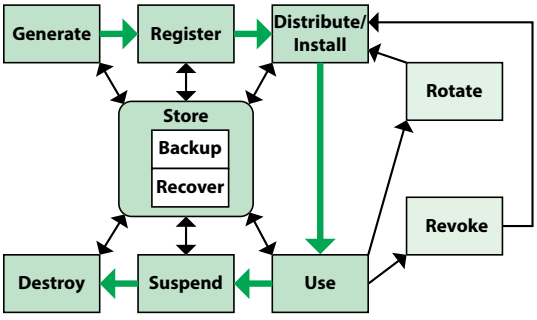


FIGURE 14.14 Cryptographic Key Life Cycle

The main cycle consists of six states:

pseudorandom number generator
A function that deterministically produces a sequence of numbers that are apparently statistically random.

- **Generate:** New keys are generated using a random or **pseudorandom number generator**. The security challenge ensures that if an attacker discovers one key in a sequence of generated keys, it is not feasible to predict future keys. Cryptographic keys should be generated with a random number generation module that is at least compliant with the SP 800-90 family of standards, which consists of:
  - **SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*:** Specifies mechanisms for the generation of random bits using deterministic methods.
  - **SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*:** Specifies the design principles and requirements for the entropy sources used by random bit generators and the tests for the validation of entropy sources. These entropy sources are intended to be combined with deterministic random bit generator mechanisms that are specified in SP 800-90A to construct random bit generators, as specified in SP 800-90C.
  - **SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*:** Specifies constructions for the implementation of random bit generators. A random bit generator may be a deterministic random bit

https://t.me/learningnets

generator or a non-deterministic random bit generator. The constructed random bit generators consist of deterministic random bit generator mechanisms, as specified in SP 800-90A, and entropy sources, as specified in SP 800-90B.

- **Register:** A new key needs to be registered or associated with a particular user, system, application, or policy.
- **Distribute/Install:** This function raises several challenging security requirements. A stored key or newly generated key must be distributed to the individual or individuals that are authorized to use it. A mutual authentication is required. The distributor of the key must be assured that the recipient is authorized for this key. The recipient must be able to trust that the key is coming from the alleged source. Finally, the act of distribution, which is accomplished only by means of a protocol over a network or a physical transfer (for example, via a USB device) needs to be performed securely.
- **Use:** In general, the use of a particular key should be restricted to a single purpose or application. Use of the same key in multiple applications expands the attack surface and increases vulnerability. In addition, a key should be used in a secure fashion that avoids disclosure.
- **Suspend:** A suspend state is needed if there is a need to retain a key beyond its operational life. For example, an entity that uses a key for data encryption must suspend use of that key when the OUP expires. However, the key may remain usable if it is needed beyond that point to decrypt data.
- **Destroy:** When a key is no longer needed, delete it from all systems containing a copy of the key, including backup and archive systems. The IT system needs to include a means, including audit trails, to determine where all copies of a key are located for this purpose.

Central to the key life cycle is a storage state. The storage must be both physically and electronically secure. Part of the security associated with a stored key is to encrypt the key. But this involves using a key-wrapping key, and its storage must be secure as well. Ideally, key-wrapping keys are stored on dedicated hardware. Two functions associated with a key storage facility are key backup and recovery. Again, the process of backup and the process of recovery must be performed in a secure fashion, and the backup storage must be secured.

https://t.me/learningnets

Two additional states are associated with keys:

- **Rotate:** The longer a key is used, the more encrypted material is potentially available to an attacker attempting to discover the key. The term *rotate* is generally used to refer to the process of replacing one key with another in accordance with the appropriate cryptoperiod policy for that key type.
- **Revoke:** If a key is compromised, or if compromise is suspected, the key must be revoked and remedial action taken. First, the need to halt the use of the key must be securely communicated to any user of the key. Second, the recovery function appropriate for the level of risk involved must be performed.

14.10 Public Key Infrastructure

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party. A PKI is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.

Before providing an overview of PKI, let's examine the concept of public key certificates.

Public Key Certificates

A *public key certificate* is a set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, called a *certification authority* (*CA*), thereby binding the public key to the entity.

Public key certificates are designed to provide a solution to the problem of public key distribution. Typically, in a public key scheme, multiple users need to have access to the public key of a given entity A, whether to encrypt data to send to A or to verify a digital signature signed by A. Each holder of a public/private key pair could simply broadcast its public key for anyone to read. The problem with this approach is that it is easy for some attacker X to impersonate A and to broadcast X's public key improperly labeled as A's public key. To counter this, it is possible to set up some trusted central authority that interacts with each user A to authenticate and then maintain a copy of A's public key. Any other user could then consult the trusted central authority over a secure, authenticated communication channel to obtain a copy of the key. It should be clear that this solution does not scale efficiently.

An alternative approach is to rely on public key certificates that are used by participants to exchange keys without contacting a public key authority in a way that is as

https://t.me/learningnets

reliable as if the keys were obtained directly from a public key authority. In essence, a certificate consists of a public key plus an identifier of the key owner, with the whole block signed by a trusted third party. Typically, the third party is a CA, such as a government agency or a financial institution, that is trusted by the user community. A user presents his or her public key to the authority in a secure manner and obtains a certificate. The user then publishes the certificate. Anyone needing this user's public key can obtain the certificate and verify that it is valid by way of the attached trusted signature. A participant also conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority.

Figure 14.15 illustrates the overall scheme for the generation of a public key certificate. The certificate for Bob's public key includes unique identifying information for Bob; Bob's public key; identifying information about the CA; and certificate information, such as expiration date. This information is then signed by computing a hash value of the information and generating a digital signature using the hash value and the CA's private key. Bob can then either broadcast this certificate to other users or attach the certificate to any document or data block he signs. Anyone who needs to use Bob's public key is assured that the public key contained in Bob's certificate is valid because the certificate is signed by the trusted CA.

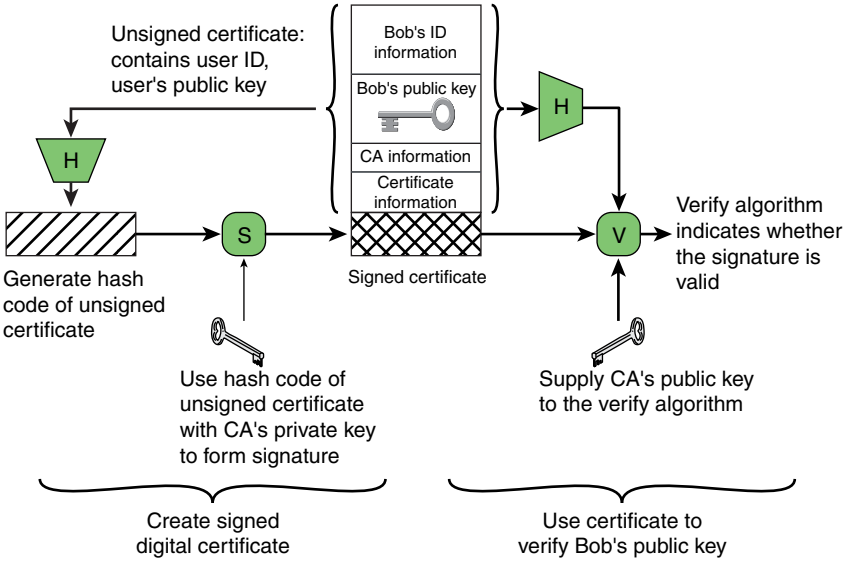


FIGURE 14.15 Public Key Certificate Use

https://t.me/learningnets

The ITU-T X.509 standard, *The Directory: Public-Key and Attribute Certificate Frameworks*, is universally accepted for formatting public key certificates.

PKI Architecture

A PKI architecture defines the organization and interrelationships among CAs and PKI users. PKI architectures satisfy the following requirements:

- Any participant can read a certificate to determine the name and public key of the certificate's owner.
- Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
- Only the certificate authority can create and update certificates.
- Any participant can verify the currency of the certificate.

Figure 14.16 shows a typical architecture for a PKI.

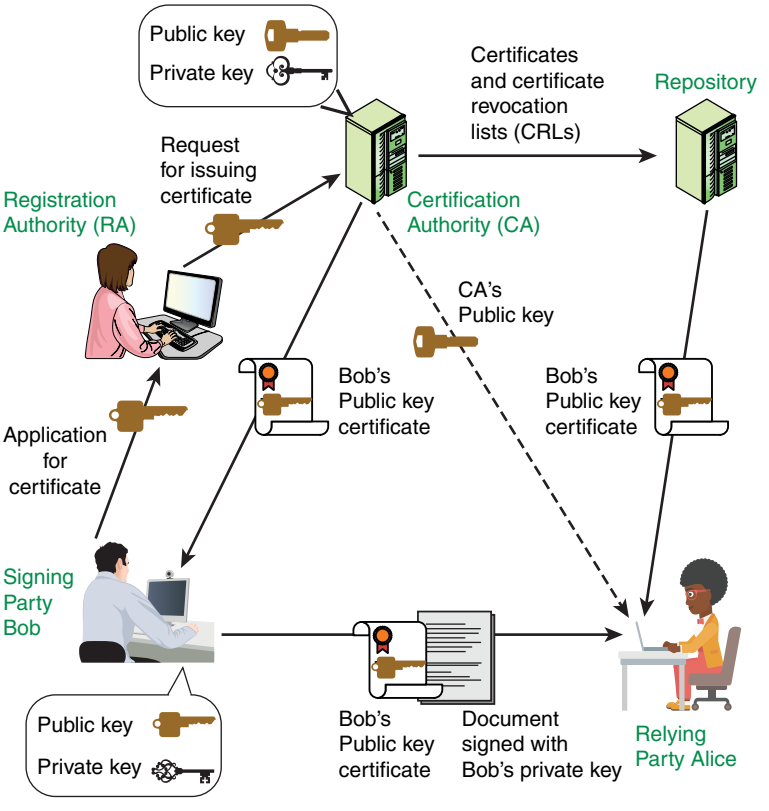


FIGURE 14.16 PKI Scenario

https://t.me/learningnets

These are the essential components of this architecture:

- **End entity:** This is either an end user; a device, such as a router or server; a process; or any item that is identified in the subject name of a public key certificate. End entities are also consumers of PKI-related services and, in some cases, providers of PKI-related services. For example, a registration authority is considered to be an end entity from the point of view of the CA.
- **Certification authority:** A CA is an authority trusted by one or more users to create and assign public key certificates. Optionally the certification authority may create the subjects' keys. CAs digitally sign public key certificates, which effectively binds the subject name to the public key. CAs are also responsible for issuing certificate revocation lists (CRLs). A CRL identifies certificates previously issued by the CA that are revoked before their expiration dates. A certificate could be revoked because the user's private key is assumed to be compromise, the user is no longer certified by this CA, or the certificate is assumed to be compromised.
- **Registration authority (RA):** An RA is an optional component that is used to offload many of the administrative functions that a CA ordinarily assumes. The RA is normally associated with the end entity registration process. This includes the verification of the identity of the end entity attempting to register with the PKI and obtain a certificate for its public key.
- **Repository:** The repository denotes any method for storing and retrieving PKI-related information, such as public key certificates and CRLs. A repository can be an X.500-based directory with client access via Lightweight Directory Access Protocol (LDAP). It can also be something simple, such as a means for retrieval of a flat file on a remote server via File Transfer Protocol (FTP) or Hypertext Transfer Protocol (HTTP).
- **Relying party:** A relying party is any user or agent that relies on the data in a certificate in making decisions.

Figure 14.16 illustrates the interactions of the various components. Consider a relying party, Alice, who needs to use Bob's public key. Alice must first obtain in a reliable secure fashion a copy of the public key of the CA. This can be done in a number of ways, depending on the particular PKI architecture and enterprise policy. If Alice wishes to send the encrypted data to Bob, Alice checks with the repository to determine if Bob's certificate was revoked, and if it wasn't, she obtains a copy of Bob's certificate. Alice can then use Bob's public key to encrypt data sent to Bob. Bob can also send to Alice a document signed with Bob's private key. Bob may include his certificate with the document or assume that Alice already has obtained or can obtain the certificate. In either case, Alice first uses the CA's public key to verify that the

https://t.me/learningnets

certificate is valid and then uses Bob's public key (obtained from the certificate) to validate Bob's signature.

Rather than using a single CA, an enterprise may need to rely on multiple CAs and multiple repositories. CAs are organized in a hierarchical fashion, with a root CA that is widely trusted signing the public key certificate of subordinate CAs. Many root certificates are embedded in web browsers so they have built-in trust of those CAs. Web servers, email clients, smartphones, and many other types of hardware and software also support PKI and contain trusted root certificates from the major CAs.

Management Issues

Deployment of a PKI is a complex task for any enterprise. NIST SP800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, suggests the following general plan:

- **Analyze data and applications:** As with any application or security service added to the enterprise architecture, PKI has security implications. The usual risk analysis should be done. In addition to comparing the initial and operating costs of the PKI with anticipated cost reductions, a cost/benefit analysis should attempt to identify larger risks due to not implementing a PKI. The analysis should also identify the data and applications that will use PKI services.
- **Review sample policies:** An efficient approach to developing a PKI is to collect sample policies and use them as templates to develop the enterprise PKI policy. A good resource for finding such policies is the OASIS PKI website. Another example is the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*.
- **Draft certificate policy:** A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. A certificate policy can help a certificate user decide whether a certificate should be trusted in a particular application. For example, a particular certificate policy might indicate applicability of a type of certificate for the authentication of electronic data interchange transactions for the trading of goods within a given price range. A useful document in this regard is RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.



OASIS PKI Website
http://www
.oasis-pki.org

https://t.me/learningnets

- **Select a PKI product or service provider:** An enterprise PKI can be partially or completely implemented in-house with proprietary or open source software. Part or all of the service can also be outsourced to a service provider. The enterprise needs to consider a range of issues, including interoperability, ease of adoption, flexibility of administration, and scalability.
- **Develop a certification practice statement:** This is a list of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (that is, requirements specified in the certificate policy or requirements specified in a contract for services).
- **Start with a pilot deployment:** Because of the complexity of a PKI, it is best to start with a limited number of users on some number of internal applications.
- **Consider cross certification issues:** It may be possible or advisable to develop certification agreements with suppliers, customers, or other entities that the enterprise interacts with. This would involve establishing a trust relationship between certain CAs in the enterprise and outside entities.

14.11 Technical Security Management Best Practices

The SGP breaks down the best practices in the technical security management category into 2 areas and 10 topics and provides detailed checklists for each topic. The areas and topics are:

- **Security solutions:** The objective of this area is to build a sound technical security infrastructure, applying security architecture principles and integrating technical security solutions covering the following topics:
  - **Security architecture:** Lists the requirements that need to be satisfied by the application of a security architecture to enable system developers and administrators to make more effective decisions and implement consistent, simple-to-use security functionality across multiple business applications and systems throughout the organization
  - **Malware protection activities:** Provides a checklist of management actions to protect against malware.
  - **Malware protection software:** Provides a checklist of management actions related to the use of malware protection software.

https://t.me/learningnets

- **Identity and access management:** Lists IAM practices that provide effective and consistent user administration, identification, authentication, and access control mechanisms throughout the organization.
- **Intrusion detection:** Lists types of intrusions that should be detected and appropriate management policies for handling intrusions. The objective is to identify suspected or actual malicious attacks and enable the organization to respond before serious damage is done.
- **Information leakage protection:** Focuses on identifying sensitive information that may be at risk of unauthorized disclosure and detection if disclosed to unauthorized individuals or systems. The topic lists management actions related to information leakage protection.
- **Digital rights management:** Lists the recommended documented standards/procedures for the provision and management of digital rights management across the organization. The objective of this topic is to ensure that the access to and processing of highly sensitive information is restricted to specific functions by a limited number of authorized individuals.

- **Cryptography:** The objective of this area is to deploy approved cryptographic solutions (for example, using encryption, public key infrastructure, digital signatures) in a consistent manner across the organization to help protect the confidentiality of information, determine whether critical information has been altered, provide strong authentication, and support non-repudiation.
  - **Cryptographic solutions:** The objective of this topic is to protect the confidentiality of sensitive information, preserve the integrity of critical information, and confirm the identity of the originator of transactions or communications. The topic recommends defining when cryptography should be used, selection of approved algorithms, and documented use of cryptographic solutions.
  - **Cryptographic key management:** The objective of this topic is to ensure that cryptographic keys are not compromised (for example, through loss, corruption, or disclosure), thereby exposing critical or sensitive information to attack. This topic provides guidance for managing keys in accordance with documented standards/procedures and in accordance with protection against unauthorized access or destruction.
  - **Public key infrastructure (PKI):** The objective of this topic is to ensure that a PKI operates as intended, is available when required, provides adequate protection of related cryptographic keys, and can be recovered in the event of an emergency. It details policies for using CAs.

https://t.me/learningnets

14.12 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms.

anomaly detection
asymmetric cryptography
brute-force attack
certification authority
ciphertext
clickless malware
cryptanalysis
cryptographic algorithm
cryptographic key management
cryptoperiod
cryptosystem (cryptographic system)
data at rest
data encryption
data in motion
data in use
data integrity
data loss prevention
decryption algorithm
demilitarized zone (DMZ)
digital rights management
digital signature
encryption algorithm
federated identity management
fileless malware
group key
hash value
host-based intrusion detection
identity and access management (IAM)
information leakage
intrusion detection
malicious software (malware)
misuse detection
network-based intrusion detection
plaintext
port mirror
Potentially Unwanted Program (PUP)
private key
pseudorandom number generator
public key
public key certificate
public key encryption
public key infrastructure
registration authority
relying party
repository
secure hash function
security architecture
single sign-on (SSO)
symmetric encryption
technical security controls
user authentication

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Explain the concept of technical security controls.
2. What is a security architecture? What are the key characteristics of a security architecture?
3. Explain the layers of the SABSA model.
4. Does the SABSA matrix provide two-way traceability? If yes, how?

https://t.me/learningnets

5. List and describe some common types of malware.
6. According to SP 800-83, what are some desired capabilities of good malware protection software?
7. What is identity and access management? How can it be deployed?
8. What are some best practices for avoiding common security mistakes with IAM?
9. What is an intrusion detection system? How may such a system be classified?
10. What are two generic approaches to intrusion detection?
11. What are some common approaches to recognizing sensitive data in real time?
12. Who/what are the principal users of a DRM system?
13. What is cryptography? How is it useful?
14. List five key ingredients of symmetric encryption.
15. What are the key ingredients of a public key encryption scheme?
16. How does the SP 800-57 standard classify key types?
17. Why should you avoid using a key for a prolonged period of time?
18. What is a public key certificate?
19. Explain the typical architectural components of a PKI system.

14.13 References

BAYL13: Baylor, K., *Top 8 DRM Best Practices*. NSS Labs Research Report. 2013. https://www.nsslabs.com/linkservid/A59EC3DC-5056-9046-9336E175181E14C9/

BURK12: Burkett, J., "Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA." *Information Security Journal*, February 15, 2012.

CIS18: Center for Internet Security. *The CIS Critical Security Controls for Effective Cyber Defense version 7.* 2018. https://www.cisecurity.org/controls/

https://t.me/learningnets

ENIS14: European Union Agency for Network and Information Security, *Algorithms, Key Size and Parameters—2014*. November 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

ENIS18: European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2017.* January 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

HEIS14c: Higher Education Information Security Council, "Identity and Access Management." *Information Security Guide*, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Identity+and+Access+Management

MAAW10: Messaging Anti-Abuse Working Group, *Overview of DNS Security—Port 53 Protection.* MAAWG Paper, June 2010. https://www.m3aawg.org

MOGU07: Mogull, R., *Understanding and Selecting a Data Loss Prevention Solution*. SANS Institute White Paper, December 3, 2007. https://securosis.com/assets/library/publications/DLP-Whitepaper.pdf

MOUL11: Moulds, R., *Key Management for Dummies.* Hoboken, NJ: Wiley, 2011.

SHER09: Sherwood, J., Clark, A., & Lynas, D., *Enterprise Security Architecture*. SABSA White Paper, 2009. http://www.sabsa.org

SHOR10: Shore, M., & Deng, X., "Architecting Survivable Networks using SABSA." *6th International Conference on Wireless Communications Networking and Mobile Computing*, 2010.

STAL17: Stallings, W., *Cryptography and Network Security.* Hoboken, NJ: Pearson, 2017.

STAL18: Stallings, W., & Brown, L., *Computer Security: Principles and Practice.* Hoboken, NJ: Pearson, 2018.

ZIND17: Zindel, A., "IAM Best Practices to Reduce Your Attack Surface." *Centrify Blog*, August 30, 2017. https://blog.centrify.com/reduce-attack-surface-iam/

https://t.me/learningnets

Chapter 15

Threat and Incident Management

What is the concept of defense: The parrying of a blow. What is its characteristic feature: Awaiting the blow.

—*On War*, Carl Von Clausewitz

Learning Objectives

After studying this chapter, you should be able to:

- Present an overview of the process of managing technical vulnerabilities.
- Appreciate the importance of security event logging to the event management process.
- Understand the nature and purpose of threat intelligence.
- Explain the typical nature of cyber attacks and strategies for preventing and responding to them.
- Understand the difference between a security event and a security incident.
- Present an overview of the security incident management process.
- Explain the specialized aspect of incident management known as digital forensics.
- Present an overview of threat and incident management best practices.

This chapter deals with detecting and responding to technical security attacks. The first four sections focus on the management of threats and vulnerabilities and the monitoring of events that may represent threats exploiting vulnerabilities. The remaining sections deal with responding to security incidents that constitute attacks or violations of security policy.

https://t.me/learningnets

15.1 Technical Vulnerability Management

Technical vulnerability management, usually referred to simply as *vulnerability management*, is a security practice specifically designed to proactively mitigate or prevent the exploitation of **technical vulnerabilities** that exist in a system or an organization. The process involves the identification, classification, remediation, and mitigation of various vulnerabilities in a system. It is an integral part of cybersecurity and is practiced together with risk management as well as other security practices.

technical vulnerability
A hardware, firmware, communication, or software flaw that leaves an information processing system open to potential exploitation either externally or internally, resulting in risk for the system.

Figure 15.1 illustrates the five key steps involved in vulnerability management. The following sections examine each off these steps in detail.

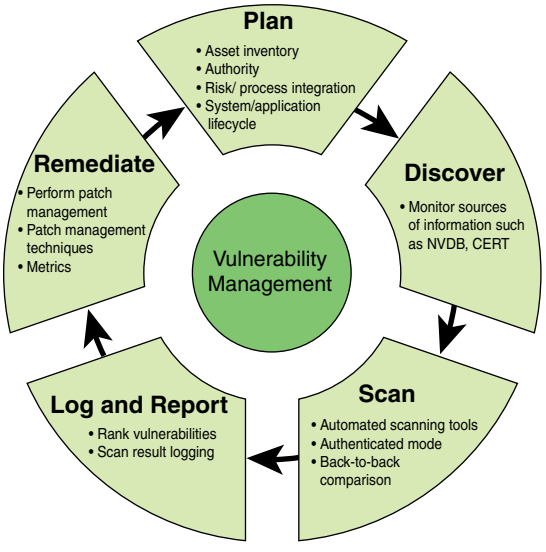


FIGURE 15.1 Vulnerability Management Steps

Plan Vulnerability Management

Effective management of technical vulnerabilities begins with planning. Key aspects of the planning process include the following:

- **Risk and process integration:** Technical vulnerability review is an operational aspect of an overall information security risk management strategy. A vulnerability analysis must consider the relative risk impacts, including those related

https://t.me/learningnets

to the potential for operational disruption. These risks must also have a clear reporting path that allows for appropriate management awareness of risk factors and exposure. Vulnerability management should also provide input into change management and incident management processes.

- **Integration with asset inventory:** As discussed in Chapter 3, "Information Risk Assessment," asset identification is an integral part of risk assessment. The resulting asset inventory allows for action to be taken once a technical vulnerability is reviewed and a mitigation strategy agreed on. By integrating the asset inventory with the vulnerability management system, an enterprise can prioritize high-risk systems where the impact of technical vulnerabilities can be greatest.
- **Establishment of clear authority to review vulnerabilities:** Because probing a network for vulnerabilities can disrupt systems and expose private data, an enterprise needs to have in place a policy and buy-in from top management before performing vulnerability assessments. The enterprise's acceptable use policy must have users and system managers consent to vulnerability scanning as a condition of connecting to the network. Awareness training should clarify that the main purpose of seeking vulnerabilities is to defend against attacks. There is also a need for policies and ethical guidelines for those who have access to data from vulnerability scans. These individuals need to understand the appropriate action when illegal materials are found on their systems during a vulnerability scan.
- **System and application life cycle integration:** The review of vulnerabilities must be integrated in system release and software development planning to ensure that potential weaknesses are identified early to both lower risks and manage costs of finding these issues prior to identified release dates.

Discover Known Vulnerabilities

The discover step involves monitoring sources of information about known vulnerabilities to hardware, software, and network equipment. Key sources of information include the following:



CERT Coordination Center https://www.sei.cmu.edu/about/divisions/cert/index.cfm

- **National Institute of Standards and Technology (NIST) National Vulnerability Database (NVDB) and Common Vulnerability Scoring System (CVSS):** This excellent source of information is discussed in some detail in Section 3.5.
- **Computer emergency response (or readiness) team (CERT):** Such a team is a cooperative venture that collects information about system vulnerabilities and disseminates it to systems managers. Hackers also routinely read CERT reports. Thus, it is important for system administrators to quickly verify and apply software patches to discovered vulnerabilities. One of the most useful

https://t.me/learningnets

of these teams is the U.S. Computer Emergency Readiness Team, which is a partnership between the Department of Homeland Security and the public and private sectors, intended to coordinate responses to security threats from the Internet. Another excellent resource is the CERT Coordination Center, which grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency. The CERT Coordination Center website provides good information on Internet security threats, vulnerabilities, and attack statistics.



Packet Storm https://packetstormsecurity.com

- **Packet Storm:** Packet Storm provides around-the-clock information and tools to help mitigate both personal data and fiscal loss on a global scale. As new information surfaces, Packet Storm releases everything immediately through its RSS (Rich Site Summary) feeds, Twitter, and Facebook.



SecurityFocus https://www.securityfocus.com

- **SecurityFocus:** This site maintains two important resources. *BugTraq* is a high-volume, full-disclosure mailing list for detailed discussion and announcement of computer security vulnerabilities. The *SecurityFocus Vulnerability Database* provides security professionals with up-to-date information on vulnerabilities for all platforms and services.
- **Internet Storm Center (ISC):** Maintained by the SANS Technology Institute, the ISC provides a free analysis and warning service to thousands of Internet users and organizations and is actively working with Internet service providers to fight back against the most malicious attackers.



Internet Storm Center https://isc.sans.edu

Scan for Vulnerabilities

In addition to monitoring vulnerability reporting services, enterprises need to regularly scan software, systems, and networks for vulnerabilities and proactively address those that are found. The Center for Internet Security (CIS) recommends the following scanning regimen [CIS18]:

- Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver a prioritized lists of the most critical vulnerabilities to each responsible system administrator, along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries, described in Section 3.5) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project, which is part of the NVDB).
- Perform vulnerability scanning in authenticated mode, either with agents running locally on each end system to analyze the security configuration or with

https://t.me/learningnets

remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans; this account should not be used for any other administrative activities, and it should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to users individually.

- Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Periodically review business risks for existing vulnerabilities to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions changed, increasing the risk.

Depending on the size and structure of the institution, the approach to vulnerability scanning can differ. Small institutions with a good understanding of IT resources throughout the enterprise can centralize vulnerability scanning. Larger institutions are more likely to have some degree of decentralization, so vulnerability scanning might be the responsibility of individual units. Some institutions have a blend of both centralized and decentralized vulnerability assessment. In any case, before starting a vulnerability scanning program, it is important to have authority to conduct the scans and to understand the targets to be scanned.

There are a number of free and commercial vulnerability scanners available for enterprise use. An example of a freeware package is the Open Vulnerability Assessment System (OpenVAS), which scans for thousands of vulnerabilities and supports concurrent scan tasks and scheduled scans. OpenVAS includes a daily updated feed of vulnerability tests. Perhaps the most widely used commercial scanner is Nessus. Nessus uses a variety of types of scans and looks for a broad range of vulnerabilities.

There are two challenges involved in scanning that an enterprise needs to address:

- **Scanning can cause disruptions.** The scanning process can impact performance. This is especially true with legacy systems, which can have problems even with simple network port scans. IT operations staff need to be in the loop. Make them aware of the importance and relevance of scans. Also, timing needs to be resolved to ensure that scanning does not conflict with regular maintenance schedules.
- **Scanning can generate huge amounts of data and numerous false positives.** Technical vulnerability management practices produce very large data sets. Accordingly, use frequent follow-up evaluations to validate the findings. Reviewing all these vulnerabilities is infeasible. Develop a vulnerability prioritization plan before initiating a large number of scans.

https://t.me/learningnets

The vulnerability prioritization plan must be aligned with the IT infrastructure and application plan to support the overall IT strategic plan; there should not be too much focus on legacy infrastructure and legacy applications that may be retired shortly.

Log and Report

When a vulnerability scan is completed, the organization should log the results so that personnel can verify the activity of the regular vulnerability scanning tools.

An organization should rank discovered vulnerabilities, such as attaching a score to each vulnerability that reflects the following:

- The skill required to exploit the vulnerability
- The availability of the exploit to potential attackers
- The privilege gained upon successful exploitation
- The risk and impact of this vulnerability if exploitation is successful

The resulting vulnerability scoring and metrics provide a valuable guide in the remediation process.

The reporting process includes keeping track of the number and risk levels of vulnerabilities discovered over time and the effectiveness of remediation efforts in removing vulnerabilities.

With respect to logging, *The CIS Critical Security Controls for Effective Cyber Defense* [CIS18] recommends that event logs be correlated with information from vulnerability scans. This has three objectives. First, verify that the activity of the regular vulnerability scanning tools is itself logged. Second, correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable. Third, monitor the scan logs to ensure that this activity is limited to the time frames of legitimate scans. This latter objective is important both because the enterprise wants to avoid conflict with other activities, such as routine maintenance, and because vulnerability scanning itself is a form of attack that must be detected.

Remediate Vulnerabilities

An organization should deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. It should apply patches to all systems—even systems that are properly air-gapped (that is, physically not accessible from the Internet).

https://t.me/learningnets

NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, provides a very detailed list of recommendations for patch management. This chapter provides a brief summary of those recommendations, which are grouped into three categories: performing patch management, patch management technologies, and patch management metrics.

Performing Patch Management

There are a number of issues to consider related to performing patch management. One is the relationship between timing, prioritization, and testing. Ideally, every discovered vulnerability should be patched as soon as discovered. But, because resources are limited, enterprises need to prioritize patching. Further, there is a risk of installing a patch throughout an enterprise without testing it, so the resources involved in testing need to be taken into account. An organization should consider the impact of a patch on operational systems, such as rebooting or changing configurations. It should also take special care if it uses multiple automated means of patching, such as self-patching software, third-party services, and network-based capability. An organization should anticipate and resolve conflicts and maintain a policy to verify that patches are effective on all relevant systems.

Patch Management Technologies

Table 15.1 shows three types of patch management techniques: agent-based scanning, agentless scanning, and passive network monitoring.

TABLE 15.1 Comparison of Patch Management Techniques

Characteristic	Agent-Based Scanning	Agentless Scanning	Passive Network Monitoring
Admin privileges needed on hosts?	Yes	Yes	No
Supports unmanaged hosts?	No	No	Yes
Supports remote hosts?	Yes	No	No
Supports appliances?	No	No	Yes
Bandwidth needed for scanning?	Minimal	Moderate to excessive	None
Potential range of applications detected?	Comprehensive	Comprehensive	Only those that generate unencrypted network traffic

https://t.me/learningnets

Details of the three patch management techniques are as follows:

- **Agent-based scanning:** Requires an agent to be running on each host to be patched, with one or more servers managing the patching process and coordinating with the agents. Each agent is responsible for determining what vulnerable software is installed on the host, communicating with the patch management servers, determining what new patches are available for the host, installing those patches, and executing any state changes needed to make the patches take effect.
- **Agentless scanning :** Uses one or more servers that perform network scanning of each host to be patched and determine what patches each host needs. Generally, agentless scanning requires that servers have administrative privileges on each host so that they can return more accurate scanning results and so they have the ability to install patches and implement state changes on the hosts.
- **Passive network monitoring:** Monitors local network traffic to identify applications (and, in some cases, operating systems) that are in need of patching. Unlike the other techniques, this technique identifies vulnerabilities on hosts that don't permit direct administrator access to the operating system, such as some Internet of Things (IoT) devices and other appliances. However, the passive monitoring must be linked to system management software that has the ability to install patches.

Common features of patch management capabilities include identifying which patches are needed, bundling and sequencing patches for distribution, allowing administrators to select which patches may or may not be deployed, and installing patches and verifying installation. Many patch management technologies also allow patches to be stored centrally (within the organization) or downloaded as needed from external sources.

A supplementary approach to traditional patch management is virtual patching. Virtual patching is implemented in a hardware device or software module that sits between incoming traffic and an application, a database, a server, or an endpoint. The virtual patch capability scans all traffic for exploits and blocks specific communications and resource usage, based on several factors. Virtual patching is an interim measure when it is difficult to immediately install needed patches.

Patch Management Metrics

As with other aspects of security, management needs metrics to evaluate the use of patch management. SP 800-40 gives the following examples of possible implementation measures:

- What percentage of the organization's desktops and laptops are being covered by the enterprise patch management technologies?

https://t.me/learningnets

- What percentage of the organization's servers have their applications automatically inventoried by the enterprise patch management technologies?

SP 800-40 gives the following examples of possible effectiveness/efficiency measures:

- How often are hosts checked for missing updates?
- How often are asset inventories for host applications updated?
- What is the minimum/average/maximum time to apply patches to X% of hosts?
- What percentage of the organization's desktops and laptops are patched within X days of patch release? Y days? Z days? (In this case, X, Y, and Z are different values, such as 10, 20, and 30.)
- On average, what percentage of hosts are fully patched at any given time? What percentage of high impact moderate impact, and low impact hosts are fully patched??
- What percentage of patches are applied fully automatically, versus partially automatically, versus manually?

SP 800-40 gives the following examples of possible impact measures:

- What cost savings has the organization achieved through its patch management processes?
- What percentage of the organization's information system budget is devoted to patch management?

15.2 Security Event Logging

This section begins with a discussion of the distinction between security events and security incidents and then examines the key objective in performing security event logging. The remainder of this section deals with details of the security event logging function.

In the information security field, a distinction is commonly made between events and incidents:

- **Security event:** An occurrence considered by an organization to have potential security implications to a system or its environment. Security events identify suspicious or anomalous activity. Events sometimes provide indications that incident are occurring.

https://t.me/learningnets

- **Security incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

A related concept is an indicator of compromise (IoC). IoCs are specific techniques used in the course of an attack, which may appear as anomalous behavior. SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, defines IoCs as forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that were compromised. IOCs for the discovery of compromised hosts include for example, the creation of registry key values. IOCs for network traffic include, for example, uniform resource locators (URLs) or protocol elements that indicate malware command-and-control servers. The rapid distribution and adoption of IOCs improve information security by reducing the time during which information systems and organizations are vulnerable to the same exploit or attack.

The term *security event* covers both events that are security incidents and those that are not, as shown in Figure 15.2.

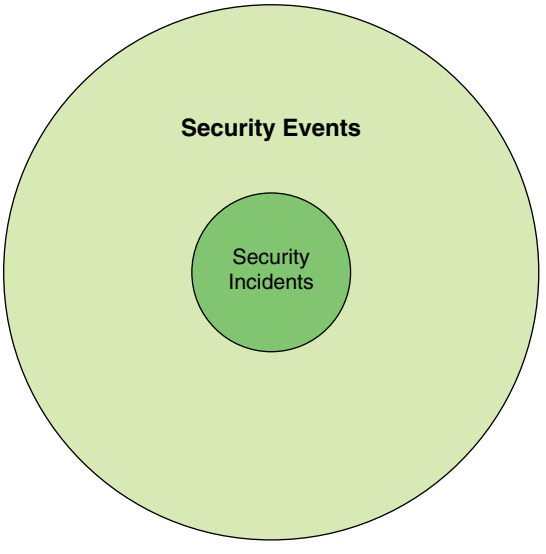


FIGURE 15.2 Security Events and Incidents

https://t.me/learningnets

In a certification authority workstation, for example, a list of security events can include the following:

- Logging an operator into or out of the system
- Performing a cryptographic operation, such as signing a digital certificate or certificate revocation list
- Performing a cryptographic card operation (creation, insertion, removal, or backup)
- Performing a digital certificate life cycle operation (rekey, renewal, revocation, or update)
- Posting a digital certificate to an X.500 directory
- Receiving a key compromise notification
- Receiving an improper certification request
- Detecting an alarm condition reported by a cryptographic module
- Failing a built-in hardware self-test or a software system integrity check

Only the final four events in this list are security incidents. This section and the following one address issues related to security events. Sections 15.6 and 15.7 discuss the management of security incidents.

Security Event Logging Objective

The objectives of security event logging are to help identify threats that may lead to an information security incident, maintain the integrity of important security-related information, and support forensic investigations. Effective logging enables an enterprise to review events, interactions, and changes that are relevant to security. With a record of events such as anomalies, unauthorized access attempts, and excessive resource usage, an enterprise can perform an analysis to determine the cause.

Potential Security Log Sources

A wide variety of sources of security events can be logged, including the following:

log
A record of the events occurring within an organization's systems and networks.

- Server and workstation operating system **logs**
- Application logs (for example, web server, database server)
- Security tool logs (for example, antivirus, change detection, intrusion detection/prevention system)

https://t.me/learningnets

- Outbound proxy logs and end-user application logs
- Firewalls and other perimeter security devices for traffic between local user and remote database or server (referred to as north–south traffic)
- Security devices between data center storage elements that communicated across a network (referred to as east–west traffic), which may involve virtual machines and software-based virtual security capabilities

The abundance of log sources present a considerable challenge to enterprise security management. An organization should create a central repository to store logs in a standardized format. This may require conversion software and consolidation software to keep the amount of log information manageable.

What to Log

In determining what types of events to log, an organization must take into consideration a number of factors, including relevant compliance obligations, institutional privacy policies, data storage costs, access control needs, and the ability to monitor and search large data sets in an appropriate time frame. The following are examples of potential security-related events that that could be logged:

- **Operating system logs:** Successful user logon/logoff; failed user logon; user account change or deletion; service failure; password changes; service started or stopped; object access denied; object access changed
- **Network device logs:** Traffic allowed through firewall, traffic blocked by firewall; bytes transferred; protocol usage; detected attack activity; user account changes; administrator access
- **Web servers:** Excessive access attempts to nonexistent files; code (for example, SQL [Structured Query Language] or HTML [Hypertext Markup Language]) seen as part of the URL; attempted access to extensions not implemented on the server; web service stopped/started/failed messages; failed user authentication; invalid request; internal server error

Protection of Log Data

An organization needs to protect log data in terms of confidentiality, data integrity, availability, and authenticated usage. Logs can contain sensitive information, such as a user's password or the content of emails. This presents security and privacy risks. In addition, if logs are altered or deleted, malicious activity might not be noticed or the identity of the malicious party might be concealed.

https://t.me/learningnets

Role-based access controls are used to partition the ability to read and modify log data based on business needs and position responsibilities.

Log Management Policy

log management
The process for generating, transmitting, storing, analyzing, archiving, and disposing of log data.

NIST SP 800-92, *Guide to Computer Security Log Management*, recommends addressing the following questions in a **log management** policy:

- Log generation:
  - Which types of hosts perform logging?
  - Which host components perform logging (for example, operating system, service, application)?
  - Which types of events each component logs (for example, security events, network connections, authentication attempts)?
  - Which data characteristics are logged for each type of event (for example, username and source IP address for authentication attempts)?
  - How frequently each type of event is logged (for example, every occurrence, once for all instances in *x* minutes, once for every *x* instances, every instance after *x* instances)?
- Log transmission:
  - Which types of hosts transfer logs to a log management infrastructure?
  - Which types of entries and data characteristics are transferred from individual hosts to a log management infrastructure?
  - How is log data transferred (for example, which protocols are permissible), including out-of-band methods, where appropriate (for example, for standalone systems)?
  - How frequently is log data transferred from individual hosts to a log management infrastructure (for example, in real time, every five minutes, every hour)?
  - How are the confidentiality, integrity, and availability of each type of log data protected while in transit, and is a separate logging network used?
- Log storage and disposal:
  - How often are logs rotated or archived?
  - How are the confidentiality, integrity, and availability of each type of log data protected while in storage (at both the system level and the application level)?

https://t.me/learningnets

- How long is each type of log data preserved (at both the system level and the infrastructure level)?
- How is unneeded log data disposed of (at both the system level and the infrastructure level)?
- How much log storage space is available (at both the system level and the infrastructure level)?
- How are log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records, handled (for example, how the impacted logs must be marked, stored, and protected)?

- Log analysis:
  - How often is each type of log data analyzed (at both the system level and the infrastructure level)?
  - Who is able to access the log data (at both the system level and the infrastructure level), and how are accesses logged?
  - What should happen when suspicious activity or an anomaly is identified?
  - How are the confidentiality, integrity, and availability of the results of log analysis (for example, alerts, reports) protected while in storage (at both the system level and the infrastructure level) and in transit?
  - How does the organization handle inadvertent disclosures of sensitive information recorded in logs, such as passwords or the contents of emails?

15.3 Security Event Management

Security event management (SEM) is the process of identifying, gathering, monitoring, analyzing, and reporting security-related events. The objective of SEM is to extract from a large volume of security events those events that qualify as incidents. SEM takes data input from all devices/nodes and other similar applications, such as log management software. The collected events data is analyzed with security algorithms and statistical computations to trace out any vulnerability, threat, or risk, as shown in Figure 15.3.

https://t.me/learningnets

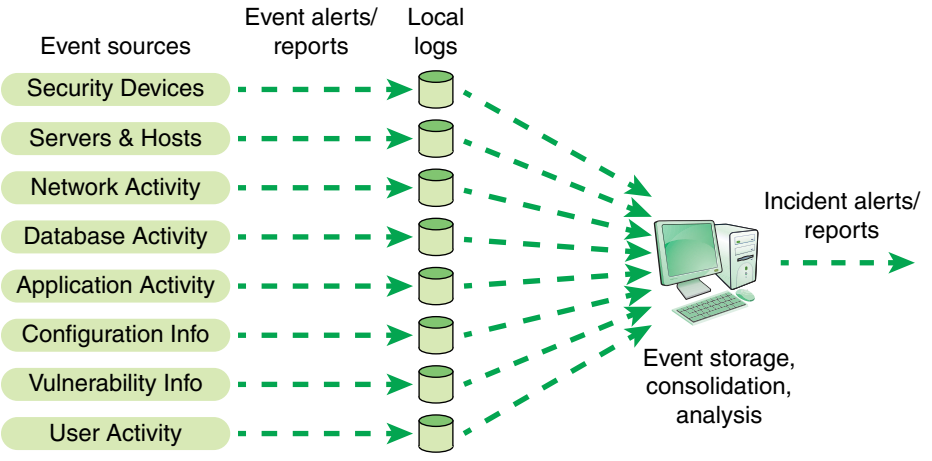


FIGURE 15.3 Security Event Management

SEM Functions

The first phase of event management is the collection of event data in the form of logs, as discussed in the preceding section. As event data are generated, they are generally stored in logs local to the devices that generate them. A number of steps need to be taken at this point:

1. **Normalization:** For effective management, the log data needs to be in a common format to enable further processing.
2. **Filtering:** This step includes assigning priorities to various types of events. On the basis of priority, large number of events can be set aside and not subject to further analysis, or they can be archived in case there is a need to review them later.
3. **Aggregation:** The IT facility of a large enterprise generates millions of events per day. It is possible to aggregate them by categories into a more manageable amount of data. For example, if a particular type of traffic is blocked a number of times, it is sufficient to record as a single aggregate event the type of traffic and the number of times it was blocked over a particular time frame.

These preliminary steps reduce the volume of data. The objective of the next steps is to analyze the data and generate alerts of security incidents.

Analysis includes the following aspects:

- **Pattern matching:** It is important to look for data patterns within the fields of stored event records. A collection of events with a given pattern can signal a security incident.

https://t.me/learningnets

- **Scan detection:** Often, an attack begins with a scan of IT resources by the attacker, such as port scans, vulnerability scans, or other types of pings. A substantial number of scans being found from a single source or a small number of sources can signal a security incident.
- **Threshold detection:** A straightforward form of analysis is the detection of a threshold being crossed. For example, if the number of occurrences of a type of event exceeds a given threshold in a certain time period, that constitutes an incident.
- **Event correlation:** Correlation consists of using multiple events from a number of sources to determine that an attack or suspicious activity occurred. For example, if a particular type of attack proceeds in multiple stages, the separate events that record those multiple activities need to be correlated in order to see the attack. Another aspect of correlation is to correlate particular events with known system vulnerabilities, which might result in a high-priority incident.

SEM Best Practices

Because SEM systems interact with virtually all other systems in an IT environment, deployment of SEM system is a large and complex project and needs to be planned and implemented carefully.

Plan

SEM planning begins with understanding the scope of the project, in the context of the enterprise. The blog post "Preparing for Security Event Management" [HUTT07] lists the following considerations in planning an SEM system:

- Depending on such factors as the complexity of the infrastructure, SEM tools, and configured pattern/logic, the deployment of an implementation can take from a month up to a year.
- The load generated by SEMS may require the use of several dedicated servers.
- The real-time nature of alerts may result is substantial volumes of data. Thus the SEM planners need to carefully consider performance and sizing requirements.
- A large, distributed installation requires careful network planning, that includes consideration of bandwidth demands and modes of failure.

https://t.me/learningnets

- Some systems require the installation of agents to relay information to SEM collectors, while others are agentless.
- Any return on investment (ROI) from SEM is proportional to the care and attention spent training analysts in its proper use.

With an understanding of the scale of a SEM project, a management team assigns responsibilities and authority for aspects of the project and determines which IT and IT security staff need to be involved in development, deployment, and use of SEM. At this point, it is important to address more specific questions about the SEM to guide acquisition and development, including the following:

- Which systems should be monitored?
- Which events are important, and what information should be collected from the local logs?
- Where should the central event log be stored, and how will it be protected and accessed?
- How long should log data be retained?
- How will the event data be analyzed to generate meaningful alerts and metrics?
- How will the performance of the SEM system be monitored?

Assess

The current security status of an IT system needs to be assessed. This involves performing a baseline vulnerability assessment on existing systems. At minimum, a team should remedy the most serious vulnerabilities for the most valuable assets. Once this is done, the team needs to assess the SEM requirements for the enterprise. The blog post "Preparing for Security Event Management" [HUTT07] lists the following objectives:

- Understand your priorities. What systems should you plug into the SEM first, and what part of your IT is subject to the most attacks?
- Determine which portions of the IT infrastructure are critical. This will dictate the level of alert level settings configure within the SEM for various IT infrastructure components.
- Determine which events are logged and which are not, as well as the level of detail of the logging for each logged event.
- Develop an inventory of all security products, their intended use, and whether or not each product is being used properly.

https://t.me/learningnets

- Understand where you need vulnerability remediation before event management. SEM software works best when used to monitor well-configured systems; it does not fix things that are currently insecure or broken.

Simplify

A simplification of the overall security infrastructure has benefits in and of itself and also makes the task of SEM easier. There are several considerations in this regard:

- Over time, the security infrastructure can contain elements that are either no longer needed because they duplicate other functions or that are configured or deployed ineffectively. Remove, reconfigure, or redeploy these elements.
- As much as feasible, retire legacy software and equipment and consolidate external routes into the enterprise network.
- Consider grouping high-value assets together for highest security.
- Deploy a default deny policy as broadly as possible. For example, perhaps only user actions that are specifically allowed are performed, and all others are prohibited. Or maybe applications on a whitelist are allowed to run, and all others are automatically blocked. Default deny makes for short and elegant configuration, fewer events that need investigation, and greater overall security.

Another aspect of simplification is to configure and deploy systems in such a way as to reduce the number of alerts and especially the number of false positives. For example, logically group servers so that sensors selectively ignore Windows attacks directed at UNIX systems and vice versa.

Deploy

The deployment of an SEM system follows the usual system development life cycle of any security project, as discussed in Chapter 8, "System Development."

15.4 Threat Intelligence

Threat intelligence, also known as *cyber threat intelligence* (*CTI*), or *cyberintelligence*, is the knowledge established as a result of analyzing information about potential or current attacks that threaten an organization. The information is taken from a number of internal and external sources, including application, system, and network logs; security products such as firewalls and intrusion detection systems; and dedicated threat feeds.

https://t.me/learningnets

Threat Taxonomy

In order to effectively use threat intelligence and respond to attacks, it is important to have a clear understanding of the types of threats faced by the enterprise. This entails understanding the potential sources of threats as well as the types of threats that may occur.

Threat Sources

The nature of threats depends to a great extent on the type of source. Threat sources can be categorized as follows:

- **Adversarial:** Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (that is, information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)
- **Accidental:** Erroneous actions taken by individuals in the course of executing their everyday responsibilities
- **Structural:** Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters
- **Environmental:** Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization

Types of Threats

A number of organizations have published taxonomies or catalogs of threat types. NIST provides a catalog consisting of 83 adversarial threat events and 18 non-adversarial threat events in SP 800-30, *Guide for Conducting Risk Assessments*. The adversarial threats are organized based on the cyber attack kill chain, discussed in Section 15.5. The non-adversarial threat events include user error, hardware failures, and environmental events. The European Union Agency for Network and Information Security (ENISA) Threat Taxonomy [ENIS16] lists 177 separate threats. The Web Application Security Consortium (WASC) Threat Classification [WASC10] lists 34 threat types. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) list 22 adversarial threats, 11 accidental threats, and 13 environmental threats; Table 15.2 shows the SGP's lists of threats.

https://t.me/learningnets

TABLE 15.2 Threats Defined in the SGP

Adversarial Threats	Accidental Threats
Session hijacking	User error (accidental)
Unauthorized access to legitimate authentication credentials	Mishandling of critical and/or sensitive information by authorized users
Exploit vulnerable authorization mechanisms	User error (negligence)
Unauthorized monitoring and/or modification of communications	Loss of information systems
Denial of service (DoS) attack	Undesirable effects of change
Exploit insecure disposal of an organization's information assets	Resource depletion
Introduce malware to information systems	Misconfiguration
Exploit misconfigured organizational information systems	Maintenance error
Exploit design or configuration issues in an organizations remote access service	Software malfunction (internally produced software)
Exploit poorly-designed network architecture	Software malfunction(externally acquired software)
Misuse of information systems	Accidental physical damage
Unauthorized physical access to information systems	**Environmental Threats**
Physical damage to or tampering with information systems	Pathogen (e.g., disease outbreak)
Theft of information system hardware	Storm (hail, thunder, blizzard)
Conduct physical attacks on organizational facilities or their supporting infrastructure	Hurricane
Unauthorized network scanning and/or probing	Tornado
Gathering publicly-available information about an organization	Earthquake
Phishing	Volcanic eruption
Insert subversive individuals into organizations	Flooding
Interpersonal manipulation	Tsunami
Exploit vulnerabilities in an organization's information systems	Fire (wild)
Compromise supplier or business partner of target organization	Power failure or fluctuation
	Damage to or loss of external communications
	Failure of environmental control systems
	Hardware malfunction or failure

phishing

A digital form of social engineering that attempts to acquire sensitive data, such as bank account numbers or passwords, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

It is useful to study these various lists to gain an appreciation of the breadth of threats confronting the enterprise.

https://t.me/learningnets

The Importance of Threat Intelligence

The primary purpose of threat intelligence is to help organizations understand the risks of the most common and severe external threats, such as **advanced persistent threats (APTs)**, **exploits**, and **zero-day threats**. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types of external threats that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself against the types of attacks that could do them the most damage.

As an example of the importance of threat intelligence, Figure 15.4, based on one in the Information Systems Audit and Control Association's (ISACA's) *Responding to Targeted Cyberattacks* [ISAC13], illustrates the impact of threat intelligence on an APT attack.

advanced persistent threat (APT)

A network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry. APTs differ from other types of attacks in their careful target selection and persistent, often stealthy, intrusion efforts over extended periods.

exploit

An attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders.

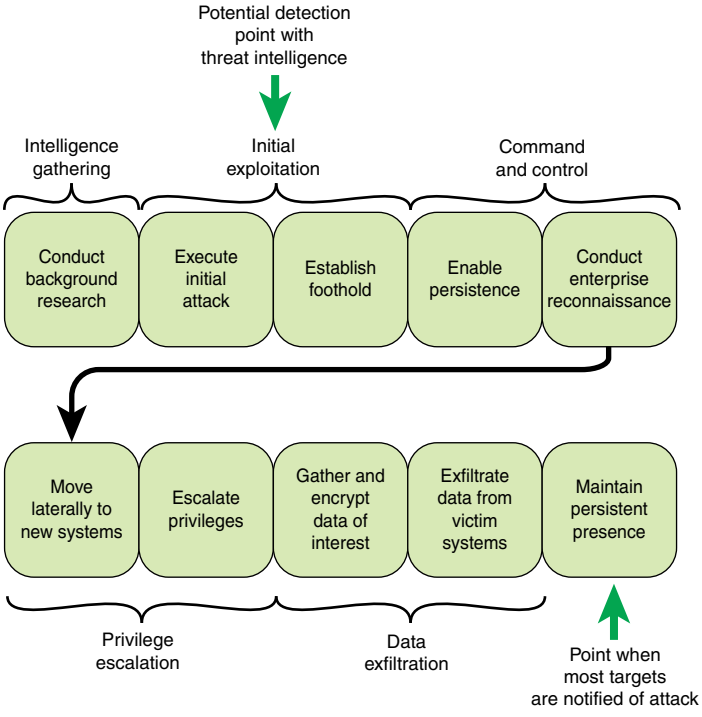


FIGURE 15.4 Potential Benefit of Threat Intelligence

A typical APT attack proceeds through the following steps:

1. **Conduct background research.** An APT attack begins with research on potential targets to identify specific avenues of attack. This maximizes the chance of the target reacting as desired.

https://t.me/learningnets

2. **Execute the initial attack.** Typically, the initial attack targets one or more specific individuals through some form of social engineering: embedding a link to malicious content into an email message, an instant message, or a social media posting or another attack vector and then persuading the target to open an attachment or click on a link to infect one or more devices with malicious software.
3. **Establish a foothold.** The APT establishes an initial foothold into the target environment by using customized malware. In almost every case, that custom software does not trigger any antivirus alert, but it does let the APT know about the successful attack. The initial infection tool, sometimes called *first-stage malware*, can have very little malicious functionality, but it generally is able to beacon home and download additional functionality, sometimes called *second-stage malware*.
4. **Enable persistence.** One of the primary objectives of the APT is to establish persistent command and control over compromised computers in the target environment—meaning control and access that survives a reboot of the targeted device and provides the APT with regular connectivity to the target environment. In most cases, this persistence is established simply by installing new services (including the attacker's command-and-control software) on the target computer that automatically start when the computer boots.
5. **Conduct enterprise reconnaissance.** After establishing persistent access to the target environment, the APT typically attempts to find the servers or storage facilities holding the targeted information. In most cases, the reconnaissance uses the tools available on the compromised computers. In some cases, the APT uploads scanning tools to search for specific types of systems (for example, identity and access management, authentication, virtual private networks [VPNs], database or email servers).
6. **Move laterally to new systems.** Part of enterprise reconnaissance necessarily includes moving laterally to new systems to explore their contents and understand the new parts of the enterprise accessed from the new systems. The APT can directly install command-and-control software on new systems to expand persistent access to the environment.
7. **Escalate privileges.** As the attackers conduct reconnaissance and move around the network using the compromised credentials of their first few targets, they inevitably seek to escalate from local user to local administrator to higher levels of privilege in the environment so that they are not constrained to any specific part of the environment. In enterprises where access to information is tightly controlled, compromising all the credentials in the environment allows the attackers to masquerade as anyone in the environment and access any resource they desire.

zero-day threat

The threat of an unknown security vulnerability in a computer software or application for which either a patch has not been released or the application developers are unaware or have not had sufficient time to address the issue. A zero-day attack is also sometimes defined as an attack that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

https://t.me/learningnets

8. **Gather and encrypt data of interest.** Having found the data of interest to the attackers, the APT generally gathers the data into an archive and then compresses and encrypts the archive. This enables the APT to hide the contents of the archive from technologies that include deep packet inspection and data loss prevention (DLP) capabilities at the enterprise boundary.
9. **Exfiltrate data from victim systems.** The APT uses a variety of tools and protocols to surreptitiously transfer data from the target systems.
10. **Maintain persistent presence.** An APT seeks to attain what its controllers have tasked it to do: maintain access to the target environment. It is not uncommon for the APT to sit undetected in an enterprise network for lengthy periods of time before being activated.

As Figure 15.4 indicates, threat intelligence enables a security team to become aware of a threat well before the point of typical notification, which is often after the real damage is done. Even if an early opportunity is lost, threat intelligence reduces the time it takes to discover that an attack has already succeeded and therefore speeds up remediation actions to limit the damage.

Gathering Threat Intelligence

The starting point for using threat intelligence is, of course, to gather that intelligence. This section looks at the wide variety of sources available to assist security personnel in this task.



Wapack Labs Cyber Threat Analysis Center http://www.wapacklabs.com/

External Sources

While it is possible to assign the threat intelligence task to one or more employees whose job it is to engage in research on existing and evolving threats, a more effective approach is to subscribe to a regular feed of threat data from a threat intelligence subscription service. One commercial example is Wapack Labs Cyber Threat Analysis Center.

There are a number of cyberintelligence vendors whose services can be employed. In addition, many of the sources of vulnerability information, such as CERTs, discussed in Section 15.1, are useful sources of threat intelligence.



National Council of ISACs https://www.nationalisacs.org

Another useful source of threat intelligence is *information sharing and analysis centers* (*ISACs*). An ISAC is a nonprofit organization, generally sector specific, that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector. In the United States, the National Council of ISACs is a central home for many ISACs. Although U.S. based, these ISACs generally have global significance.

https://t.me/learningnets

Internal Sources

Various activities in the IT infrastructure of an enterprise signal that an attack is imminent or that a threat is developing. The SGP lists the following examples:

- Event logs from technical infrastructure, such as operating system logs (for example, from servers and mobile devices; authentication and DNS [Domain Name System] logs; service and application logs; and network device logs)
- Alerts from security systems such as firewalls, malware protection, DLP, network-based intrusion detection systems (NIDSs), gateway proxy servers, and physical security systems
- Direct feeds from security event management utilities, such as those produced by security event logging software or a **security information and event management (SIEM)** system
- Dedicated teams that perform information security–related activities (for example, those responsible for incident management, IT help desk functions, and forensic investigations)
- Business support functions (for example, legal, human resources, audit, physical security, facilities)

security information and event management (SIEM)
An application or set of tools that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

Threat Analysis

Threat analysis includes the task of describing the type of possible attacks, potential attackers, and their methods of attack and the consequences of successful attacks. It involves the following:

- Identifying the vulnerabilities of the system
- Analyzing the likelihood of threats aimed at exploiting these vulnerabilities
- Assessing the consequences that would occur if each threat were to be successfully carried out
- Estimating the cost of each attack
- Costing out potential countermeasures
- Selecting the security mechanisms that are justified (possibly by using cost/benefit analysis)

An organization should carry out this analysis as a regular part of risk management. Then, when the security team is alerted to a new threat, there is already a plan in place to deal with that threat. If the threat is one that has not been anticipated, then

https://t.me/learningnets

the previously mentioned analytical steps need to be carried out with reference to this new threat.

15.5 Cyber Attack Protection

The *National Information Assurance Glossary* [CNSS10] defines *cyber attack* as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Attack Kill Chain

The concept of a cyber attack kill chain was introduced in Chapter 3 and is illustrated in Figure 15.5. Note that APTs, discussed earlier in this chapter, are a form of cyber attack (refer to Figure 15.4). The following sections consider each of the phases of a cyber attack kill chain in turn.

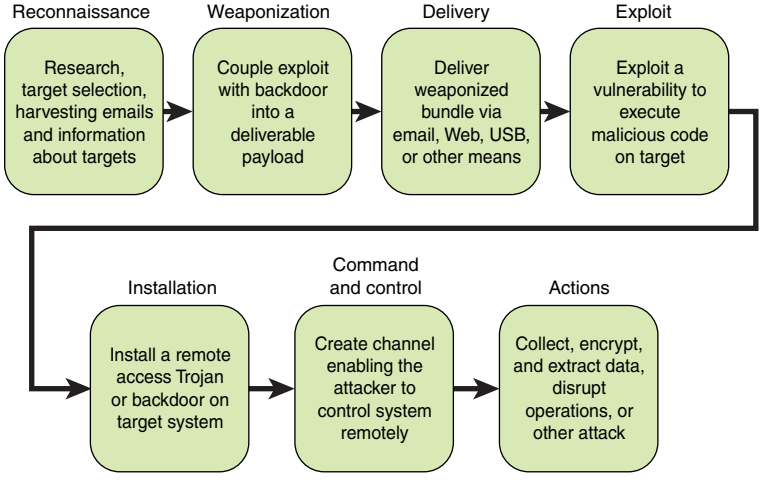


FIGURE 15.5 Cyber Attack Kill Chain

Reconnaissance

In the first stage of a typical cyber attack, the attacker decides whether the potential target is in fact a promising target and, if so, the best means of attack. Ideally, the attacker looks for a target that exhibits both serious vulnerabilities and valuable data. If the target is particularly high value, the attacker can attempt the attack even if there are few vulnerabilities.

https://t.me/learningnets

There are a number of potential sources of information about a target:

- **Names and contact details of employees online:** Even if these are not provided on the enterprise website, they may be available through social networks. This information may be used for **social engineering** purposes.
- **Details about enterprise web servers or physical locations online:** These details are used for social engineering or to narrow down a list of possible exploits that could be used break into the enterprise's environment.
- **Emails and other network traffic:** This information may be used for social engineering or to gain insight into possible avenues of attack.

social engineering
The process of attempting to trick someone into revealing information (for example, a password) or performing an action that can be used to attack an enterprise or into performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

The means of performing reconnaissance include the following:

- Perform perimeter network reconnaissance/scanning
- Perform network sniffing of exposed networks
- Gather information using open source discovery of organizational information
- Perform surveillance of targeted organizations over time to examine and assess organizations and ascertain points of vulnerability
- Perform malware-directed internal reconnaissance

Weaponization

At this stage, an attacker prepares an attack payload and crafts a tool to deliver the attack, using the gathered information. This step happens at the attacker side, without contact with the victim.

SP 800-30 lists the following types of attack tools:

- Phishing attacks
- **Spear phishing** attacks
- Attacks specifically based on deployed information technology environment
- Counterfeit/spoof website
- Counterfeit certificates

spear phishing
Phishing that is targeted against a group, a company, or individuals within a company.

https://t.me/learningnets

Delivery

During the delivery phase, the attacker sends the malicious payload to the victim by one of many intrusion methods. Possible methods of delivery include email, web traffic, instant messaging, and File Transfer Protocol (FTP). The payload can also be placed on removable media (for example, flash drives) and social engineering techniques can be used to persuade an employee to install the malware from the media to the enterprise's information systems. SP 800-30 lists a number of other delivery techniques, including the following:

- Insert malware into common freeware, shareware, or commercial IT products. This technique does not target a specific organization but is a way to find targets of opportunity.
- Insert malware into organizational information systems and information system components (for example, commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
- Replace critical information system components with modified or corrupted components. This is done through the supply chain, a subverted insider, or some combination thereof.
- Place individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.

Exploit

During the exploit phase, the delivered payload is triggered and takes action on the target system to exploit a vulnerability. This phase is concerned with gaining entry to the system in order to begin the actual attack. This phase can make use of a vulnerability known to the attacker, or the initially delivered payload can search for and discover vulnerabilities that enable continuing and expanding the attack.

A wide variety of attacks are possible at this stage, encompassing all the threat categories discussed in this book (for example, exfiltrating data, modifying data, compromising availability).

Installation

During the installation phase, the attacker installs components that permit permanent control of the target system. The objective is to mount further attacks on the enterprise. At this stage, the attacker can also elevate user privileges of installed malware and install persistent payload.

https://t.me/learningnets

Command and Control

The attacker creates a command-and-control channel in order to continue to operate the internal assets remotely. This step is relatively generic and relevant throughout the attack, not only when malware is installed. Among other actions at this stage, the adversary can take actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations. The adversary can adapt behavior in response to surveillance and organizational security measures.

Actions

The attacker performs the steps to achieve his or her goals inside the victim's network—to obtain information, destroy information, or disrupt systems or networks. This can be an elaborate active attack process that takes months and thousands of small steps to achieve.

Protection and Response Measures

The following sections describe the steps an organization can take to reduce its vulnerability to each of the phases of the cyber attack kill chain described in the preceding section.

Dealing with the Reconnaissance Phase

A number of techniques can be used to detect reconnaissance attempts. For websites, **web analytics** can detect behavior that is more in line with an attacker than a benign user. For any type of traffic, scanning the source IP addresses for those with known bad reputations is fruitful. Multiple events occurring from the same address in a small time frame may indicate a reconnaissance effort.

web analytics
The process of analyzing the behavior of visitors to a website. This process involves extracting and categorizing qualitative and quantitative data to identify and analyze onsite and offsite patterns and trends.

Prevention methods include the use of firewalls, especially if a default deny policy is used, whitelisting, and segmenting enterprise networks.

Dealing with the Weaponization Phase

As defined here, *weaponization* is a process that occurs at the attacker site and thus cannot be detected by the target. However, rapid patching and updating in addition to a regular routine of vulnerability fixing can thwart a weaponization effort by eliminating the vulnerability before it is exploited. This highlights the necessity of obtaining and acting on threat intelligence in a timely manner.

Dealing with the Delivery Phase

They key to preventing delivery is to maintain a robust security training and awareness program so that social engineering efforts are more likely to fail.

https://t.me/learningnets

A variety of technical tools are used to prevent delivery, including the following:

- **Antivirus software:** Antivirus software is a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. It is important to continuously run antivirus software to identify, trap, and destroy incoming known viruses. If a virus is detected, the antivirus software is configured to trigger a scan of the rest of the IT infrastructure for indicators of compromise associated with this outbreak.
- **Firewall:** A firewall blocks delivery attempts from known or suspected hostile sources.
- **Web application firewall (WAF):** As described in Chapter 9, "Business Applications Management," a WAF is a firewall that monitors, filters, or blocks data packets as they travel to and from a web application.
- **Intrusion prevention system (IPS):** An IPS is a system that detects an intrusive activity and also attempts to stop the activity—ideally before it reaches its targets. It is similar to an intrusion detection system but is proactive in attempting to block the intrusion.

Dealing with the Exploit Phase

Countermeasures at the exploit stage include the following:

- **Host-based intrusion detection systems (HIDS):** Once an exploit is inside the enterprise network and attacking hosts, a HIDS detects and alerts on such attempts.
- **Regular patching:** Patching discovered vulnerabilities helps contain the damage.
- **Data restoration from backups:** Once an exploit is discovered and removed, it may be necessary to restore a valid copy of data from a backup.

Dealing with the Installation Phase

Tools that detect suspicious software or behavior, such as antivirus software and HIDS, are appropriate at the installation stage. These tools include specific actions such as the following:

- An organization should remediate any malware infections as quickly as possible before they progress. Scan the rest of the enterprise network for indicators of compromise associated with this outbreak.

https://t.me/learningnets

- Sometimes a **distributed denial-of-service (DDoS) attack** is used to divert attention away from another, more serious, attack attempt. Increase monitoring, investigate all related activity, and work closely with the enterprise Internet service provider (ISP) or other service provider.
- An organization should detect, monitor, and investigate unauthorized access attempts, giving priority to those that are mission critical and/or contain sensitive data.
- An organization should identify the privileged user accounts for all domains, servers, apps, and critical devices. Monitoring should be enabled for all systems, and for all system events, and the monitoring system should feed the log monitoring infrastructure.
- An organization should configure critical systems to record all privileged escalation events and set alarms for unauthorized privilege escalation attempts.

distributed denial-of-service (DDoS) attack
A DoS attack in which multiple systems are used to flood servers with traffic in an attempt to overwhelm available resources (transmission capacity, memory, processing power, and so on), making them unavailable to respond to legitimate users.

Dealing with the Command-and-Control Phase

Countermeasures at the command-and-control stage include the following:

- **Network-based intrusion detection systems (NIDS):** A NIDS can detect and alert on attempts to use an unauthorized or suspicious channel.
- **Firewall:** A firewall blocks communication with known or suspected hostile sources and also blocks suspicious activity or packet content.
- **Tarpit:** This is a service on a computer system (usually a server) that delays incoming connections for as long as possible. Tarpits were developed as a defense against computer worms, based on the idea that network abuses such as spamming or broad scanning are less effective if they take too long. A tarpit is used for incoming traffic that is not on an approved source whitelist.

Dealing with the Actions Phase

If an attack gets to the stage of ongoing advanced attacks, a critical aspect of security is a backup policy. An organization should regularly back up all critical data and systems; test, document, and update system recovery procedures; and, during a system compromise, capture evidence carefully and document all recovery steps as well as all evidentiary data collected.

Incident management, discussed in Sections 15.6 and 15.7, is relevant for this stage.

https://t.me/learningnets

Non-Malware Attacks

An increasingly important category of cyber attacks is referred to as *non-malware attacks*. The chief characteristic of a non-malware attack is that it does not involve downloading any malicious files or code onto target devices. Rather, the attacker uses existing software on target machines, whitelisted applications, and authorized protocols to carry out malicious activities. Non-malware attacks can appear at several points along the cyber kill chain. Among the most common types of non-malware attacks are the following:

- Remote logins
- **Windows Management Instrumentation (WMI)**–based attacks
- **PowerShell**-based attacks
- Attacks leveraging Office macros

Windows Management Instrumentation (WMI)

A protocol to pull system metadata from Microsoft Windows devices, most notably operating system and software version data.

PowerShell

A scripting language and related facilities that provides rich access to Window systems, including access to security settings.

When dealing with security events other than malware, the difficulty of automating the process of responding is significantly greater. When antivirus software or other incident monitoring software encounters malware, the malware can be automatically removed or isolated for further analysis. But an intrusion or another indicator of compromise may require both automated tools for recognition and human involvement for response. The article "Restoring Machine Learning's Good Name in Cybersecurity" [CHES17] gives the following example: For a typical scenario in a medium-to-large company, the security analyst's procedure for confronting a potential breach consists of the following:

- Identify a security event.
- Try to identify the attack intent based on the event name and description (which is rarely satisfactory, as the event name is usually too generic and the description too vague to accurately represent the intent).
- Search for and collect relevant, potentially useful data from third-party threat centers, security blogs, intelligence reports, and similar sources.
- Begin analyzing data.
- Determine event intent and possible impact on the organization, based on associated threat information.

But an analyst's job doesn't end there. All such events in an organization must be aggregated in an effort to find cause-and-effect correlations to reveal potential coordinated attack campaigns. When there are numerous security events to process in a short time, which is typical, the task becomes impossible.

https://t.me/learningnets

An increasingly popular approach to overcoming this problem is to use artificial intelligence (AI) and machine learning (ML) software:

- **Artificial intelligence:** Technology that appears to emulate human performance, typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogs with people, enhancing human cognitive performance (also known as cognitive computing), or replacing people on execution of nonroutine tasks. AI implies the capability to learn and adapt through experience and to come up with solutions to problems without using rigid, predefined algorithms, which is the approach of non-AI software.
- **Machine learning:** AI software that modifies its own algorithms in order to become more intelligent and improve future results. Unlike the static logic ("if this, do that") in regular programs, machine learning continues to refine its logic so that the next operation is more effective than the preceding one.

A number of vendors now offer ML and AI products to support cyber response efforts. However, this technology has not reached the level of maturity required to significantly improve protection. A recent report by Carbon Black [CARB17] aggregates insight from more than 400 interviews with leading cybersecurity researchers, summarized as follows:

- Non-malware attacks are considered more threatening than malware- based attacks.
- Non-malware attacks are increasingly leveraging native system tools, such as WMI and PowerShell, to conduct nefarious actions.
- Confidence in the ability of legacy antivirus software to prevent non-malware attacks is low.
- AI is considered by most security researchers to be in its nascent stages and not yet able to replace human decision making in cybersecurity.
- Researchers say attackers can bypass ML-driven security solutions.
- Cybersecurity talent, resourcing, and trust in executives continue to be top challenges plaguing many businesses.

15.6 Security Incident Management Framework

The ISO 27000 suite defines *information security incident management* as consisting of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents. This section examines the management

https://t.me/learningnets

framework for security information management, which comprises the relevant individuals, information, and tools required by the organization's information security incident management process. Figure 15.6 highlights the four key elements of an incident response framework, which are discussed subsequently in this section. The purpose of the framework is to ensure the availability of resources that are required to help resolve information security incidents quickly and effectively. Section 15.7 examines the security incident management process.

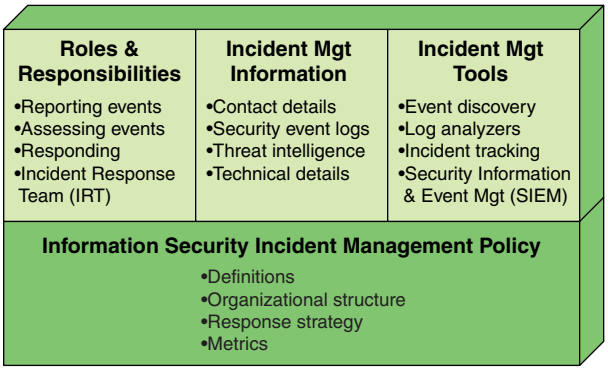


FIGURE 15.6 Security Information Management Framework

A number of standards are relevant to the implementation of security incident management, including the following:

- **ISO 27002, *Code of Practice for Information Security Controls*:** Provides a comprehensive checklist of management practices for incident response.
- **ISO 27035-1, *Information Security Incident Management—Part 1: Principles of Incident Management*:** Presents basic concepts and phases of information security incident management and how to improve incident management. This part combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents and applying lessons learned.
- **ISO 27035-2, *Information Security Incident Management—Part 2: Guidelines to Plan and Prepare for Incident Response*:** Describes how to plan and prepare for incident response. Provides a very detailed discussion of what should go into an information security incident management plan.
- **ITU-T X.1056, *Security Incident Management Guidelines for Telecommunications Organizations*:** Provides practical guidance on how to respond to incidents effectively and efficiently.

https://t.me/learningnets

- **NIST SP 800-61, *Computer Security Incident Handling Guide*:** Provides detailed guidance for planning, managing, and implementing an incident response plan.
- **RFC 2350, *Expectations for Computer Security Incident Response*:** Describes issues and requirements for managing incident response.

It is the responsibility of the security managers to review all these documents.

Objectives of Incident Management

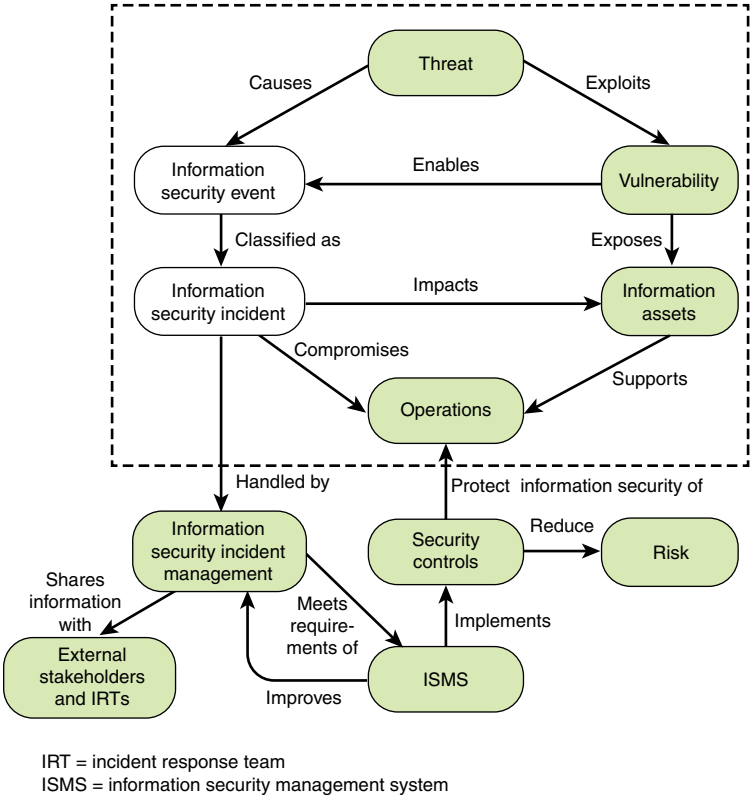
ISO 27035-1 lists the following as the objectives for security incident management:

- Information security events are detected and dealt with efficiently, in particular deciding when they are to be classified as information security incidents.
- Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
- The adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response.
- A link is established with relevant elements from crisis management and business continuity management through an escalation process.
- Information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents.
- Lessons are learned quickly from information security incidents, vulnerabilities, and their management. This feedback mechanism increases the chances of preventing future information security incidents from occurring, improves the implementation and use of information security controls, and improves the overall information security incident management plan.

Relationship to Information Security Management System

Figure 15.7, adapted from figures in ISO 27035-1, indicates the relationship between information security incident management and an information security management system (ISMS) (refer to Figure 2.1). The upper part of the figure, bounded by dashed lines, illustrates the relationships among objects in an information security incident. A threat causes a security event by exploiting a vulnerability, which enables the threat to create the event. The event is potentially an incident that impacts information assets exposed by vulnerabilities and compromises the operations supported by the information assets. In the upper part of the figure, the shaded objects are preexisting and affected by the unshaded objects.

https://t.me/learningnets



IRT = incident response team
ISMS = information security management system

FIGURE 15.7 Security Incident Management in Relation to ISMS and Applied Controls

The lower part of Figure 15.7 indicates the bigger picture, showing how security incident management relates to risk management and an ISMS.

Incident Management Policy

Essential to successful incident management is a documented incident management policy. Such a policy should have sections that deal with overall management, including the following topics:

- A specification of internal and external interested parties
- An agreed-on definition of *incident* and guidelines to identify a security incident
- A definition of *incident response/handling* and its overall objectives and scope
- A statement of management intent, supporting the goals and principles of incident response/handling

https://t.me/learningnets

- A brief explanation of the incident response/handling policies, principles, standards, and compliance requirements that are of particular importance to the enterprise
- A definition of general and specific responsibilities for incident response/handling, including handling of evidence and reporting
- References to documentation that supports the policy, such as detailed incident response/handling, incident triage, and computer forensic policies and procedures
- User awareness training pertaining to incident identification and reporting
- Metrics for measuring the incident response capability and its effectiveness

The policy should also cover the strategy for dealing with incidents, including the following topics:

- Identification of an incident and response (for example, shutdown, containment, quarantine)
- Acquisition of volatile and static data
- Retention and analysis of data
- Remediation
- Referral to law enforcement
- Handling of forensic data
- Escalation of incidents
- Reporting of findings
- Definition of the learning process from incidents to upgrade systems and processes

Roles and Responsibilities

The information security incident management framework defines the roles and responsibilities of the information security incident management team and others involved in responding to incidents. ISO 27035-2 lists the following incident management responsibilities for which personnel need to be assigned:

- Detecting and reporting information security events. (This is the responsibility of any permanent or contracted personnel in an organization and its companies.)
- Assessing and responding to information security events and incidents and being involved in post-incident resolution activities. These activities include learning

https://t.me/learningnets

and improving information security and the information security incident management plan itself. These activities are the responsibility of members of the point of contact team, the incident response team, management, public relations personnel, and legal representatives.

- Reporting information security vulnerabilities and dealing with them. (This is the responsibility of any permanent or contracted personnel in an organization and its companies.)

Most organizations want to create a formal *information security incident response team* (*IRT*). X.1056 defines an IRT as a team of appropriately skilled and trusted members of the organization, which handles security incidents during their life cycle. At times, external experts may supplement this team. Members of the team should have the following backgrounds/skill sets:

- Understanding of known threats, attack signatures, and vulnerabilities
- Understanding of the enterprise network, security infrastructure, and platforms
- Experience in security response and/or troubleshooting techniques
- Experience in forensic techniques and best practices
- Understanding of regulations and laws as they pertain to privacy and disclosure and evidentiary requirements
- Understanding of systems, threats, and vulnerabilities, and remediation methods in their area of business responsibility

Part-time or liaison members of the IRT should be well versed in the following key areas:

- Information technology
- Information security
- Corporate communications
- Human resources
- Legal
- Business unit management and technology specialists
- Corporate security (including physical security)

The IRT's primary responsibility is to respond to incidents throughout the incident response life cycle, as described in Section 15.7. The IRT is also involved in making recommendations for improving security practices and implementing new security controls.

https://t.me/learningnets

Incident Management Information

The information security incident management framework is responsible for detailing the types of information needed to assist information security incident management. The SGP lists the following information types needed for incident management:

- Contact details for relevant parties, such as business managers, technical experts (such as those in a security operations center [SOC] or equivalent), and external suppliers
- Security-related event logs (for example, those produced by applications, systems, network devices, and security products)
- Details about affected business environments, such as processes, operations, and applications
- Technical details, such as network diagrams, system configurations, and external network connections
- Threat intelligence and the results of threat analysis

Incident Management Tools

The information security information management framework specifies the tools needed to assist information security incident management (for example, checklists, e-discovery software, log analyzers, incident tracking software, forensic analysis software).

One of the most important incident management tools is a SIEM system. SIEM is a broader term than SEM and refers to a more comprehensive system of information collection and subsequent action. Capabilities of a typical SIEM include the following, according to ISACA's *Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives* [ISAC10]:

- **Data collection:** In a typical use case, a SIEM solution must be able to touch a number of different systems: firewalls, proxy servers, databases, intrusion detection and prevention systems, operating systems, routers, switches, access control systems, and so on. Some of these share similar logging and alert functions, but frequently there is significant variation in the format, protocol, and information provided.
- **Data aggregation:** The aggregator serves as a consolidating resource before data is sent to be correlated or retained.
- **Data normalization:** Normalization is the process of resolving different representations of the same types of data into a similar format in a common database.

https://t.me/learningnets

- **Correlation:** Event correlation is the function of linking multiple security events or alerts, typically within a given time window and across multiple systems, to identify anomalous activity that is not evident from any singular event.
- **Alerting:** When data that trigger certain responses (such as alerts or potential security problems) are gathered or identified, SIEM tools activate certain protocols to alert users, such as notifications sent to the dashboard, an automated email, or text message.
- **Reporting/compliance:** Protocols in a SIEM are established to automatically collect data necessary for compliance with company, organizational, and government policies. Both custom reporting and report templates (generally for common regulations such as the Payment Card Industry Data Security Standard [PCI DSS] and the U.S. Sarbanes-Oxley Act) are typically part of a SIEM solution.
- **Forensics:** The ability to search log and alert data for indicators of malicious or otherwise anomalous activities is the forensic function of the SIEM. Forensics, which is supported by the event correlation and normalization processes, requires highly customizable and detailed query capabilities and drill-down access to raw log files and archival data. Working in concert, these technologies greatly enhance the investigative capabilities of security analysts, just as data collection, aggregation, and correlation technologies enhance their ability to detect and respond to real-time events.
- **Retention:** Data need to be stored for long periods so that decisions can be made based on more complete data sets.
- **Dashboards:** Dashboards are used to analyze and visualize data in an attempt to recognize patterns or target activity or data that do not fit into a normal pattern.

15.7 Security Incident Management Process

Many organizations react in an ad hoc manner when a security incident occurs. Because of the potential cost of security incidents, it is cost-beneficial to develop a standing capability for quick discovery and response to such incidents. This capability also serves to support the analysis of past security incidents with a view to improving the ability to prevent and respond to incidents.

SP 800-61 defines a four-phase incident management process, as shown in Figure 15.8, that serves as a useful way of structuring the discussion.

https://t.me/learningnets

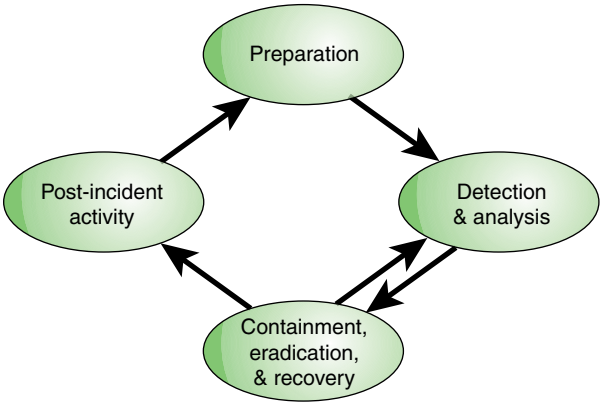


FIGURE 15.8 Incident Response Life Cycle

Preparing for Incident Response

An effective incident response capability requires the participation of a number of people within the organization. Making the right planning and implementation decisions is key to establishing a successful incident response program. Tasks involved in preparing for incident response include the following:

- Develop an organization-specific definition of the term *incident* so that the scope of the term is clear
- Create an incident response policy
- Develop incident response and reporting procedures
- Establish guidelines for communicating with external parties
- Define the services that will be provided by the IRT
- Select an organizational structure and staffing model for incident response
- Staff and train the IRT
- Establish and maintain accurate notification mechanisms
- Develop written guidelines for prioritizing incidents
- Have a plan for the collection, formatting, organization, storage, and retention of incident data

https://t.me/learningnets

Detection and Analysis

Perhaps the most challenging phase of the incident response life cycle is detection and analysis, which consists of determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

Incident Detection

Sections 15.2 and 15.3 discuss event logging and management in some detail. As part of the incident response life cycle, security incidents must be detected from among the numerous security events logged and recorded.

Key aspects of incident detection include the following:

- All IT personnel and users need to be trained and comfortable regarding procedures for reporting failures, weaknesses, and suspected incidents; methods to recognize and detect problems with security protections; and how to escalate reporting appropriately.
- Technical controls must be implemented for the automated detection of security incidents from event logs, coupled with reporting that is as near real time as possible. Key technical tools include IDSs and continuously monitoring antivirus software.
- Situational awareness information needs to be collected from internal and external data sources, including local system and network traffic and activity logs; news feeds concerning ongoing political, social, or economic activities that might impact incident activity; and external feeds on incident trends, new attack vectors, current attack indicators, and new mitigation strategies and technologies.
- Digital evidence needs to be gathered and stored securely, and its secure preservation must be continually monitored in case the evidence is required for legal prosecution or internal disciplinary action.

Analysis

Once an incident is detected, it is appropriate to move immediately to the next phase of the life cycle, which deals with removing the threat and recovery from any damage. Most enterprises choose to do a more in-depth analysis at this point. Typical actions include the following:

https://t.me/learningnets

- Determine the magnitude of the impact. Consider the number of users affected or the number of devices or the segments of the network.
- Assess the severity. What is the sensitivity of the data involved? What is the criticality of the service, or system, or application? What is the potential for damage or liability?
- Assess the urgency of the event. Is it an active problem, a threat, or an event-in-progress? Was the problem discovered after the fact? Is the intrusion dormant or completed? Does this involve use of an account rather than a system? Does this involve the safety or privacy of individuals?

The analysis also needs to determine whether immediate action is needed to remove the vulnerability or to block the action that enabled the incident to occur. Such analysis may also be part of the post-incident activity phase.

Containment, Eradication, and Recovery

The containment, eradication, and recovery phase is the central task of incident management. If prevention measures failed and an incident occurs, the enterprise needs to stop the attack if it is ongoing and recover from the attack. Actions taken during this phase can conceivably uncover another incident, which feeds back to the detection and analysis phase, as shown in Figure 15.8.

Containment

Most incidents require some sort of containment. The objective is to prevent the spread of the effects of the incident before they overwhelm resources or in some other way increase damage.

Strategies for dealing with various types of incidents must be planned well in advance. The strategy varies depending on the type of incident. For example, email-borne virus, DoS attacks, and intrusion coupled with escalation of privileges require different strategies. In some cases, a system may need to be isolated from the network until it is cleaned. User or system-level accounts may need to be disabled or changed. Active sessions may need to be terminated.

The nature of the strategy and the magnitude of resources devoted to containment depends on criteria developed ahead of time. Examples of criteria include potential damage to and theft of resources, the need to preserve evidence, the effectiveness of the strategy, the time and resources needed to implement the strategy, and the duration of the solution.

https://t.me/learningnets

Eradication

Once the ongoing damage has been stopped, it may be necessary to perform some sort of eradication to eliminate any residual elements of the incident, such as malware and compromised user accounts.

Recovery

During recovery, IT personnel restore systems to normal operation to the extent possible and, if applicable, harden systems to prevent similar incidents. Possible actions include the following:

- Restoring systems with clean versions from the latest backup
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (for example, firewall rule sets)

Post-Incident Activity

Incident logging capability allows for recording incidents and notes about an incident. After an incident is dealt with in the containment, eradication, and recovery phase, the organization should initiate an evaluation process. This includes lessons-learned meetings and after-action reports. Depending on the type of incident and the security policy, a comprehensive forensic investigation may be warranted, as discussed in Section 15.9, or a comprehensive loss analysis may be undertaken.

Once the incident, its effects, and the magnitude of the effort required to recover are reviewed and analyzed, further action may be needed, such as the following:

- The incident handling process should be reviewed to determine whether the process must be modified and/or more resources committed. Such changes depend on the novelty and severity of the incident.
- Policy and process changes may be warranted. Questions to consider include the following: Were any procedures missing, were communications unclear, or were any stakeholders not appropriately considered? Did the technical staff have appropriate resources (information as well as equipment) to perform the analysis and/or the recovery?

https://t.me/learningnets

- Other improvements outside the incident management process may be needed, including new or revised technical security controls, updates to awareness and acceptable use policies, and improvements in the areas of threat intelligence and vulnerability assessment.

Table 15.3, from SP 800-61, is a useful checklist for assuring implementation of all phases of the incident response life cycle.

TABLE 15.3 Incident Handling Checklist

Detection and Analysis	
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (for example, search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (for example, new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
Post-Incident Activity	
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)

https://t.me/learningnets

15.8 Emergency Fixes

Security incident emergencies must be handled with a greater sense of urgency than other security incidents. An emergency response may entail making an emergency fix to temporarily eliminate ongoing damage until a more permanent response is provided. Implementing an emergency fix can also require that an information security officer be temporarily given access privileges not normally authorized.

To get a feel for what constitutes an emergency, consider a classification scheme for security incidents suggested in ISO 27035:

- **Emergency:** Severe impact. These are incidents that:
  - Act on especially important information systems and
  - Result in especially serious business loss or
  - Lead to especially important social impact
- **Critical:** Medium impact. These are incidents that:
  - Act on especially important information systems or important information systems and
  - Result in serious business loss or
  - Lead to important social impact
- **Warning:** Low impact. These are incidents that:
  - Act on especially important information systems or ordinary information systems and
  - Result in considerable business loss or
  - Lead to considerable social impact
- **Information:** No impact. These are incidents that:
  - Act on ordinary information systems and
  - Result in minor business loss or no business loss or
  - Lead to minor social impact or no social impact

Table 15.4 provides examples of the types of security incidents that can result in different levels of impact.

https://t.me/learningnets

TABLE 15.4 Examples of Incident Categories and Severity Classes

	Severity Class			
Incident Category	**Information**	**Warning**	**Critical**	**Emergency**
Technical attacks	Failed attempts	Single ordinary (user compromise)	Multiple (user compromise) (application privileged access compromise)	Mass (application privileged access compromise)
Technical attacks		Annoyance (scratch the surface)	Disturbance (throughput impact)	Unavailability (stop in service)
Malware	Single known (detected and blocked by antivirus protection)	Single unknown	Multiple infections Server infections	Mass infections

A security policy should include a section related to contingency plans for security incidents that require emergency fixes. It should include the following:

- Procedures for determining that an emergency fix is required
- Emergency contact information
- A summary of methods to be used related to hardware
- A summary of methods to be used related to software
- Procedures for approving emergency fixes and for logging the incident
- Procedures for revoking any emergency access required for the fix
- Procedures for documenting the incident, reviewing the response, and removing the fix
- A list of assets and resources that are most important to protect, with relative priorities assigned

A key aspect of responding to an emergency incident is that one or more individuals must have the authority to make fixes. Security officers must order emergency actions to protect information assets and override administrator privileges and roles to allow emergency access. A good security practice is to share system administrator access privileges with someone other than the system administrator, if for no other reason than to have emergency system access if the administrator is unavailable. But, having

https://t.me/learningnets

said this, such total access also requires total accountability and must be limited to the fewest number of staff necessary to keep the system secure because each person with total system access has the ability to override any and all security features.

15.9 Forensic Investigations

NIST SP 800-96, *Guide to Integrating Forensic Techniques into Incident Response*, defines computer forensics, or digital forensics, as the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Computer forensics seeks to answer several critical questions, including the following:

- What happened?
- When did the events occur?
- In what order did the events occur?
- What was the cause of these events?
- Who caused these events to occur?
- What enabled these events to take place?
- What was affected? How much was it affected?

Computer forensic analysis is used for a number of reasons, including the following:

- To investigate crimes
- To investigate suspicious employee behavior
- To reconstruct serious security incidents
- To troubleshoot operational problems
- To support due diligence for audit record maintenance
- To recover from accidental system damage

Most security incidents do not require a forensic investigation but are dealt with using the ordinary incident management process. However, more serious incidents can warrant the more in-depth analysis of a forensic investigation. For example, if an external party such as a customer or supplier suffers a loss as a result of an incident involving the enterprise, forensic analysis can help the enterprise avoid or mitigate liability. As another example, when an employee is fired as a result of an incident but claims that his or her dismissal was unfair or unfounded, improperly processed

https://t.me/learningnets

evidence can make it more difficult to justify the decision and defend against the unfair dismissal claims. Without evidence, the enterprise could be in a potentially costly situation if the employee sues.

Figure 15.9 illustrates the typical phases in the digital forensics process, which are discussed in detail in the following sections.

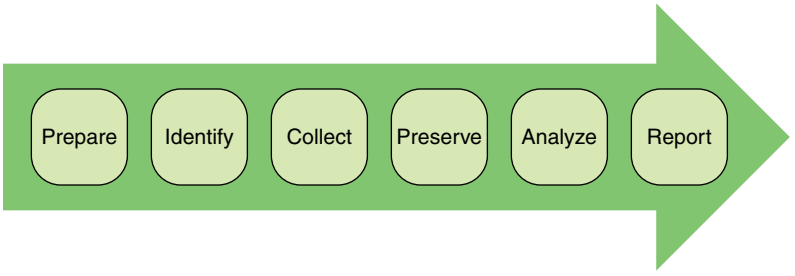


FIGURE 15.9 Phases of Digital Forensics Process

Prepare

Preparation involves the planning and policy-making activities related to forensic investigation. A section of the security policy should deal with computer forensics. SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, recommends the following considerations:

- Ensure that policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures
- Create and maintain procedures and guidelines for performing forensic tasks, based on the organization's policies and all applicable laws and regulations
- Ensure that policies and procedures support the reasonable and appropriate use of forensic tools
- Ensure that IT professionals are prepared to participate in forensic activities

In addition, an organization should establish guidelines on how to manage evidence. Such guidelines help ensure that evidence is preserved throughout the entire investigation process.

The preparation phase also covers other activities, such as staff training, staff recruitment, tool validation, and quality assurance measures.

https://t.me/learningnets

A vital aspect of preparation is to ensure that the data sources needed for forensic analysis are created and securely stored. Key actions include the following:

- Creating a file system baseline to help detect changes
- Utilizing a central system log server
- Maintaining network-level logging at key control points on the network
- Synchronizing system clocks and log timestamps using central **Network Time Protocol (NTP)** servers for systems that generate logs
- Maintaining protocol activity tables, which are useful when responding to certain types of incidents

Network Time Protocol (NTP)
A protocol that assures accurate local timekeeping on computer systems, network devices, and other system components, with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

The advantage of creating centralized logs is that they are easier to protect than local logs distributed throughout the network, which present a greater attack surface.

Identify

The identification phase is initiated when there is a request for a forensic analysis. This phase involves understanding the purpose of the request and the scope of the investigation, such as type of case, subjects involved, and system involved. A forensic analyst must determine if a request contains sufficient information to start the process. If not, the analyst must coordinate with the requester to determine the next step.

The identification phase determines where the data of interest are stored and what data can be recovered and retrieved. Another task of this phase is to set up and validate forensic hardware and software and create system configuration as needed.

Collect

Once the location or locations of data are identified, the forensic process needs to ensure that the data are collected in a manner that preserves the integrity of the evidence. Typically, enterprise policy requires the use of special-purpose forensic hardware and software to ensure that the original data are never altered and that the evidence collected stands up to legal scrutiny. Once the data are collected, they are verified and backed up to ensure that a valid image exists.

The data collection process includes one or more of the following, depending on the purpose of the forensic analysis:

- Capturing data from system logs, event logs, and incident logs
- Discovering data on computer systems
- Recovering deleted, encrypted, or damaged file information

https://t.me/learningnets

- Monitoring online activity
- Making a bit-image copy of an affected system's hard drive
- Detecting violations of corporate policy

For this phase, as well as the preservation phase, an organization should use forensic software tools that are well known in the computer forensics community, such as Forensic Tool Kit (FTK) and EnCase.

Preserve

Several actions comprise the preservation of data process, including the following:

- Creating a log that documents when, from where, how, and by whom data were collected
- Storing the data in a secure fashion to prevent tampering or contamination
- Logging each access to the data made for forensic analysis

Analyze

Analysis depends on the specifics of each job. The examiner usually provides feedback to the client during analysis, and from this dialogue the analysis may take a different path or be narrowed to specific areas.

Examples of analysis tasks include:

- Checking for changes to the system such as new programs, files, services, and users
- Looking at running processes and open ports for anomalous behavior
- Checking for Trojan horse programs and toolkits
- Checking for other malware
- Looking for illegal content
- Looking for indicators of compromise
- Determining the who, when, where, what, and how details of a security incident

Numerous forensic analysis tool can assist an analyst, including the following:

- Disk and data capture tools
- File viewers

https://t.me/learningnets

- File analysis tools
- Registry analysis tools
- Internet analysis tools
- Email analysis tools
- Mobile devices analysis tools
- macOS analysis tools
- Network forensic tools
- Database forensic tools



NIST Computer Forensics Tool Testing Program https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

A helpful resource is the NIST Computer Forensics Tool Testing Program. This program tests available forensic tools and maintains a catalog. It enables practitioners to find tools that meet their specific technical needs. The catalog provides the ability to search by technical parameters based on specific digital forensics functions, such as disk imaging or deleted file recovery.

Report

The nature of any report resulting from a forensic investigation depends on the original purpose of the investigation. In general, SP 800-86 lists the following factors that affect reporting for any type of investigation:

- **Alternative explanations:** The available information may not provide a definitive explanation of the cause and nature of an incident. The analyst should present the best possible conclusions and highlight alternative explanations.
- **Audience consideration:** An incident requiring law enforcement involvement requires highly detailed reports of all information gathered and can also require copies of all evidentiary data obtained. A system administrator might want to see network traffic and related statistics in great detail. Senior management might simply want a high-level overview of what happened, such as a simplified visual representation of how the attack occurred and what should be done to prevent similar incidents.
- **Actionable information:** Reporting also includes identifying actionable information gained from data that allows an analyst to collect new sources of information. For example, a list of contacts may be developed from the data that can lead to additional information about an incident or a crime. Also, information that is obtained might help prevent future events, such as learning about a backdoor on a system that is to be used for future attacks, a crime that is being planned, a worm scheduled to start spreading at a certain time, or a vulnerability that could be exploited.

https://t.me/learningnets

15.10 Threat and Incident Management Best Practices

The SGP breaks down the best practices in the threat and incident management category into two areas and nine topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Cybersecurity resilience:** The objective of this area is to manage threats and vulnerabilities associated with business applications, systems, and networks by scanning for technical vulnerabilities, maintaining up-to-date patch levels, performing continuous security event monitoring, acting on threat intelligence, and protecting information against targeted cyber attacks.
  - **Technical vulnerability management:** This topic deals with establishing a process for the identification and remediation of technical vulnerabilities in business applications, systems, equipment, and devices. The objective is to address technical vulnerabilities quickly and effectively, thus reducing the likelihood of their being exploited and preventing serious security incidents.
  - **Security event logging:** This topic deals with procedures for recording security-related events in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis.
  - **Security event management:** This topic deals with management guidelines for reviewing and analyzing security-related event logs. The objective is to detect known vulnerabilities, detect unusual or suspicious activity, and respond to events that need to be investigated in a timely manner.
  - **Threat intelligence:** The objective of this topic is to promote situational awareness about current and emerging threats, supporting information risk-related decisions and activities, based on analysis of a range of sources. The SGP discusses internal and external sources of threat information, details that should be included in threat information, analysis policy, and threat intelligence sharing.
  - **Cyber attack protection:** This topic provides checklists for protecting enterprise assets during all phases of a cyber attack.
- **Security incident management:** The objective of this area is to develop a comprehensive and documented strategy for managing security incidents, which is supported by a process for the identification, response, recovery, and post-implementation review of information security incidents.

https://t.me/learningnets

- **Security incident management framework:** This topic lists considerations for defining an information security incident management framework, including relevant individuals, information, and tools required by the organization's information security incident management process.
- **Security incident management process:** This topic provides a checklist of actions related to detecting, analyzing, containing, recovering from, and learning from security incidents.
- **Emergency fixes:** This topic provides a checklist of actions for applying emergency fixes, responding to emergencies in a timely and secure manner, and reducing disruption to the organization.
- **Forensic investigations:** This topic provides a checklist of actions for dealing with information security incidents or other events (for example, e-discovery requests) that require forensic investigation.

15.11 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

advanced persistent threat (APT)
antivirus software
computer emergency response team (CERT)
cyber attack
cyber attack kill chain
cyber threat intelligence
distributed denial-of-service (DDoS) attack
emergency fix
exploit
forensics
incident response team (IRT)
information sharing and analysis center (ISAC)
log
log management
Network Time Protocol (NTP)
patch
patch management
phishing
PowerShell
security event
security event management
security incident
security incident management
security information and event management (SIEM)
social engineering
spear phishing
tarpit
technical vulnerability
technical vulnerability management
threat intelligence
web analytics
Windows Management Instrumentation (WMI)
zero-day threat

https://t.me/learningnets

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Explain the term *technical vulnerability*. What are five key steps involved in vulnerability management?
2. What are key sources for discovering vulnerabilities?
3. Describe two difficulties, or challenges, that result from the use of vulnerability scans
4. What are some of the common patch management techniques used in organizations?
5. Differentiate between a *security event* and a *security incident*.
6. For security event logging, what events should be captured in operating system logs, network device logs, and web server logs?
7. What kind of analysis can you do on cleaned SEM data?
8. How can you categorize threat sources?
9. Briefly describe an APT attack and list the steps in a typical APT attack.
10. What are the steps to prevent delivery of malicious payload in a cyber attack kill chain?
11. For protecting against cyberattack exploits, list and briefly describe three countermeasures
12. According to ISO 27035-1, what are the objectives for security incident management?
13. What are some key capabilities of a typical SIEM?
14. According to ISO 27035, how are security incidents classified?
15. Explain typical phases in the digital forensics process.

15.12 References

CARB17: Carbon Black, *Beyond the Hype: Security Experts Weigh in on Artificial Intelligence, Machine Learning, and Non-malware Attacks.* March 2017. https://www.carbonblack.com/wp-content/uploads/2017/03/Carbon_Black_Research_Report_NonMalwareAttacks_ArtificialIntelligence_MachineLearning_BeyondtheHype.pdf

https://t.me/learningnets

CHES17: Chesla, A., "Restoring Machine Learning's Good Name in Cybersecurity." *Forbes Community Voice*, July 25, 2017. https://www.forbes.com/sites/forbestechcouncil/2017/07/25/restoring-machine-learnings-good-name-in-cybersecurity/#18be0e1168f4

CIS18: Center for Internet Security. *The CIS Critical Security Controls for Effective Cyber Defense version 7.* 2018. https://www.cisecurity.org

CNSS10: Committee on National Security Systems. *National Information Assurance (IA) Glossary.* April 2010.

ENIS16: European Union Agency for Network and Information Security, *ENISA Threat Taxonomy—A Tool for Structuring Threat Information.* January 2016. https://www.enisa.europa.eu

HUTT07: Hutton, N., "Preparing for Security Event Management." 360is Blog, February 28, 2017. http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf

ISAC10: ISACA, *Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives*. 2008. www.isaca.org

ISAC13: ISACA, *Responding to Targeted Cyberattacks.* 2008. www.isaca.org

WASC10: Web Application Security Consortium, *WASC Threat Classification*. January 2010. http://www.webappsec.org/

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Chapter 16

Local Environment Management

"No ticket! Dear me, Watson, this is really very singular. According to my experience it is not possible to reach the platform of a Metropolitan train without exhibiting one's ticket."

—*The Adventure of the Bruce-Partington Plans*, by Sir Arthur Conan Doyle

Learning Objectives

After studying this chapter, you should be able to:

- Discuss the issues relevant to local environment security.
- Provide an overview of various types of physical security threats.
- Assess the value of various physical security prevention and mitigation measures.
- Discuss measures for recovering from physical security breaches.
- Understand the value of the SP 800-53 physical security controls.
- Present an overview of local environment management best practices.

This chapter discusses security issues specific to local environments physically separate from other local environments that together comprise the physical assets of an organization. Section 16.1 addresses issues related to local information processing security issues, how to characterize and address these issues, and how to coordinate and integrate local security policies with the overall enterprise security policy. Section 16.2 looks at physical security.

16.1 Local Environment Security

An enterprise devotes much of its effort in developing security policies and procedures to addressing enterprisewide security issues. However, when there are multiple locations for IT assets and end

https://t.me/learningnets

users, it is equally important to consider the unique security challenges of each **local environment**. The following are some of the factors that require the development of strategies tailored to the local environment:

local environment
In the context of cybersecurity, a physically distinct and separate area, which may be a single office space, building, or building complex. The local environment may have unique physical security, personnel security, and information security requirements that are distinct from those of the rest of the enterprise.

- Most organizations have many different end-user environments, often across physical locations and comprising individuals who use a wide range of technologies to handle information.
- There are significant differences in the knowledge, behavior, and actions of end users in different environments.
- End users employ a variety of corporate-issued and personally owned devices (in organizations that have bring your own device [BYOD] policies).
- End users sometimes blur the boundaries between work and personal computing (for example, with mobile computing).
- End users typically want to configure their own user environments and install personal software such as applications for social networking, instant messaging, peer-to-peer networking, and voice over IP (VoIP).

Any approach to addressing security issues in the local environment must be mindful of corporate goals such as worker empowerment, increased functionality and utility, and the ability of end users to control their environment. Further, end users may have the clout to resist security efforts that they view as being overly restrictive or costly.

Dealing with this complex challenge involves two steps:

1. Enterprise security officers need to understand the unique security issues associated with end-user environments in the organization.
2. The enterprise needs to task one or more individuals in each local environment with tailoring and implementing enterprise security policy locally.

Local Environment Profile

Security management and senior executives may not have a good grasp on the security issues in a local environment, such as the value of information that employees have access to and use, the threats this information is exposed to when not adequately protected, and the potential business impact if this information is compromised in the end-user environment.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) recommends that, for each distinct local environment, a responsible

https://t.me/learningnets

security officer or group should develop a security profile. Key elements of the profile include:

- **Individuals:** Each local environment should have one or more staff members with specific information security responsibilities, as discussed subsequently. The profile should detail the types of users at the location, in terms of their application and data usage, level of security awareness training, security privileges, and whether they use mobile devices and, if so, what type.
- **Business processes and information:** This area includes the types of information used and whether any sensitive information is accessible. The profile should include descriptions of business processes that involve user information access, as well as descriptions of any external suppliers (for example, cloud service providers).
- **Technology use:** This topic comprises the applications and IT equipment used.
- **Location:** The profile should provide a description of the location housing the users and equipment. The profile should indicate to what degree the location is accessible to the public or to others who are not part of the organization, whether the physical space is shared with other organizations (for example, an office building or park), and any particular environmental hazards (for example, tornado zone).

Local Security Coordination

An enterprise must manage the twofold concern of ensuring that the enterprisewide information security policy is applied in the local environment and that policy elements are adapted to the local profile. For this purpose, each location should have one or more individuals responsible for addressing these concerns. The types of individual roles required include an information security coordinator and an information protection champion.

Information Security Coordinator

An information security coordinator is responsible for developing and maintaining information security in the local environment and coordinating this with the organization's security executives and managers. The information security coordinator should be responsible for the following:

- Developing the local environment profile
- Determining the best way to implement enterprise security policy in the local environment

https://t.me/learningnets

- Providing oversight of implementation of the information security policy in the local environment
- Ensuring that physical security arrangements are in place and adequate
- Assisting with communicating security policies and requirements to local end users and local management
- Keeping enterprise security executives and management informed of security-related developments
- Overseeing or coordinating end-user awareness training
- Coordinating area response to information security risk assessments
- Coordinating area response to information security risk audit requests, as directed
- Ensuring completion and submission of required documentation

Information Protection Champion

In recent years, a number of enterprises have adopted the practice of designating an *information protection champion*, or *security champion*, in each local environment. The information security coordinator may take on this role, or there may be a separate individual in each local environment. Security management may appoint someone to this role or may include it in the job description of a specific role, such as that of a security coordinator, or it can be offered as a volunteer opportunity.

COBIT 5 recommends the use of champions and indicates that their role is to promote a culture of security throughout the organization. On the one hand, the champion acts as an ambassador for the chief information security officer (CISO) and the enterprise security manager to communicate security policy in the local environment. On the other hand, the champion acts as an advocate for a security culture, promoting awareness and working to ensure that security requirements are built into end-user systems and software.

The Information Systems Audit and Control Association (ISACA) report *Creating a Culture of Security* [ISAC11] recommends the use of security champions to promote an intentional culture of security. Implicit in the use of the term *intentional* is that enterprises do not, for the most part, have an effective culture of security, one that supports the protection of information while also supporting the broader aims of the enterprise. They must take active, directed steps to improve it, and security champions can assist in developing that culture in end-user environments.

The SGP lists the following as tasks for the information protection champion:

- Identifying critical and sensitive information
- Assessing information risks in the local environment

https://t.me/learningnets

- Selecting and implementing security controls to mitigate information risks
- Delivering information security awareness messages to promote information security in the local environment
- Managing actual and suspected information security incidents

16.2 Physical Security

For information systems, the role of physical security is to protect the physical assets that support the storage and processing of information. Physical security involves two complementary requirements. First, physical security must prevent damage to the physical infrastructure that sustains the information system. In broad terms, that infrastructure includes the following:

- **Information system hardware:** This includes data processing and storage equipment, transmission and networking facilities, supporting documentation, and offline storage media.
- **Physical facility:** The physical facility is the buildings and other structures housing the system and network components.
- **Supporting facilities:** These facilities underpin the operation of the information system. This category includes electrical power, communication services, and environmental controls (heat, humidity, and so on).
- **Personnel:** Personnel are the humans involved in the control, maintenance, and use of the information systems.

Second, physical security must prevent misuse of the physical infrastructure that leads to the misuse or damage of the protected information. The misuse of the physical infrastructure may be either accidental or malicious (for example, vandalism, sabotage, theft of equipment, theft by copying, theft of services, unauthorized entry).

Physical Security Threats

The issues that physical security threats encompass are different for every different site and organization. Accordingly, this section provides only a general treatment. Threats to physical security can be grouped into the following categories:

- Environmental threats
- Technical threats
- Human-caused threats

https://t.me/learningnets

Environmental Threats

Environmental threats are threats that arise from natural or human-caused disasters in the physical environment of a facility. Environmental threats include the following categories:

- **Natural disasters:** Natural disasters are the source of a wide range of environmental threats to data centers, other information processing facilities, and personnel. These are potentially the most catastrophic of physical threats.
- **Inappropriate temperature/humidity:** Computers and related equipment are designed to operate within a certain temperature range. Most computer systems should be kept between 10 and 32 degrees Celsius (50 and 90 degrees Fahrenheit). Outside this range, although resources may continue to operate, they might produce undesirable results. If the ambient temperature around a computer gets too high, the computer cannot adequately cool itself, and internal components can be damaged. In addition, both high and very low humidity can result in malfunction or damage to IT equipment.
- **Fire and smoke:** Fire is a serious threat to human life and property. The threat is not only from direct flame but also from heat, release of toxic fumes, water damage from fire suppression, and smoke damage. Further, fire can disrupt utilities, especially electricity. The most common fire threat is from fires that originate within a facility. In certain locations, wildfires are also a threat.
- **Water:** Water and other stored liquids in proximity to computer equipment pose an obvious threat. The primary danger is electrical short. Moving water, such as in plumbing, and weather-created water from rain, snow, and ice also pose threats. Less common, but more catastrophic, is floodwater; much of the damage comes from the suspended material in the water. Floodwater leaves a muddy residue that is extraordinarily difficult to clean up.
- **Chemical, radiological, and biological hazards:** Chemical, radiological, and biological hazards pose a growing threat, both from intentional attack and from accidental discharge. In general, the primary risk of these hazards is to personnel. Radiation and chemical agents can also cause damage to electronic equipment.
- **Dust:** Dust is a prevalent threat that is often overlooked. Even fibers from fabric and paper are abrasive and mildly conductive, although generally equipment is resistant to such contaminants. Larger influxes of dust result from a number of incidents, such as a controlled explosion of a nearby building and a windstorm carrying debris from a wildfire. A more likely source of influx comes from dust surges that originate within the building due to construction or maintenance work.

https://t.me/learningnets

- **Infestation:** One of the less pleasant physical threats is infestation, which covers a broad range of living organisms, including mold, insects, and rodents. High-humidity conditions can lead to the growth of mold and mildew, which is harmful to both personnel and equipment. Insects, particularly those that attack wood and paper, are also a common threat, although generally not to electronic equipment.

Table 16.1 lists six categories of natural disasters, the typical warning time for each event, whether personnel evacuation is indicated or possible, and the typical duration of each event. It is possible to assess the risk of various types of natural disasters and take suitable precautions in order to prevent catastrophic loss due to natural disasters.

TABLE 16.1 Characteristics of Natural Disasters

Type of Disaster	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief (usually minutes in a single location) but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief (usually minutes in a single location) duration; threat of continued aftershocks
Ice storm/ blizzard	Several days of warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Single strike is very brief but may recur
Flood	Several days of warning generally expected	May be unable to evacuate	Site may be isolated for an extended period

Technical Threats

The two main technical threats to physical security relate to electrical power and electromagnetic radiation.

Electrical power is essential to the operation of IT equipment. All the electrical and electronic devices in the system require power, and most require uninterrupted utility power. Power utility problems can be broadly grouped into three categories:

- **Undervoltage and power outages:** Undervoltage events range from temporary dips in the voltage supply, to brownouts (prolonged undervoltage), to power outages.

https://t.me/learningnets

- **Overvoltage:** Far more serious is an overvoltage condition. A surge of voltage may be caused by a utility company supply anomaly, by some internal (to the building) wiring fault, or by lightning. The damage depends on the intensity and duration, as well as the effectiveness of any surge protectors between IT equipment and the source of the surge.
- **Noise:** Power lines are also a conduit for *noise*. In many cases, these spurious signals endure through the filtering circuitry of the power supply and interfere with signals inside electronic devices, causing logical errors.

Noise along a power supply line is only one source of electromagnetic interference (EMI). Motors, fans, heavy equipment, and even other computers generate electrical noise that can cause intermittent problems with a computer. This noise is transmitted through space as well as through nearby power lines. Another source of EMI is high-intensity emissions from nearby commercial radio stations and microwave relay antennas. Even low-intensity devices, such as cellphones, interfere with sensitive electronic equipment.

Human-Caused Physical Threats

Human-caused, or induced, threats are more difficult to deal with than environmental and technical threats. They are less predictable than other types of physical threats. Worse, human-caused threats are specifically designed to overcome prevention measures and/or seek the most vulnerable point of attack. Such threats fall into the following categories:

- **Unauthorized physical access:** Information assets such as servers, mainframe computers, network equipment, and storage networks are generally located in restricted areas, with access limited to a small number of employees. Unauthorized physical access can lead to other threats, such as theft, vandalism, or misuse.
- **Theft:** This threat includes theft of equipment and theft of data by copying. Eavesdropping and wiretapping also fall into this category. Theft can be at the hands of an outsider who has gained unauthorized access or by an insider.
- **Vandalism and industrial sabotage:** This threat includes deliberate and intended destruction of equipment and data.

Physical Security Officer

An organization should designate one person as the physical security officer (PSO). The PSO role may not be a full-time responsibility but an additional role for another staff member. The PSO is responsible for the overall implementation and management

https://t.me/learningnets

of physical security controls across an organization, including integration with applicable information security controls. As information security programs are developed, senior enterprise officials should work to ensure this coordination of complementary controls. Each local environment should also assign an employee with local PSO responsibility to coordinate with and report to the enterprise PSO.

The tasks of the PSO and his or her team include the following:

- Assessing local physical security needs by conducting physical security surveys
- Recommending physical security considerations in preparation for the construction projects, including the design phase
- Ensuring that security considerations are included in new construction, renovation, modification efforts, or lease acquisition
- Monitoring resource management (money and personnel) of the local physical security program
- In coordination with the appropriate financial officers, planning and programming necessary resources for physical security projects in the budget cycle
- Monitoring the funding status of all physical security program resource requirements
- Developing, promulgating, implementing, and monitoring the organization's physical security programs, to include appropriate controls for local environments
- Ensuring organizational implementation and monitoring of access controls (for example, authorization, access, visitor control, transmission medium, display medium, logging)
- Coordinating organizational environmental controls (for example, ongoing and emergency power support and backups, fire protection, temperature and humidity controls, water damage)
- Overseeing and managing controls for delivery and removal of assets

Defense in Depth

An important strategy seen through this book is the use of multiple overlapping protection approaches addressing the people, technology, and operational aspects of information systems. By using multiple overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. This approach is often used to provide multiple barriers between an adversary and protected information or services. This strategy is often referred to as

https://t.me/learningnets

defense in depth. One example of this strategy is multifactor authentication (refer to Figure 10.3); another is the combined use of firewalls, intrusion detection systems, and access control systems.

defense in depth
A strategy that involves constructing a system's security architecture with layered and complementary security mechanisms and countermeasures so that if one security mechanism is defeated, one or more other mechanisms (which are "behind" or "beneath" the first mechanism) still provide protection.

The defense in depth strategy is equally appropriate and effective for physical security. Protective measures include fences, gates, locked doors, electronic access (such as via smart card), armed guards, surveillance systems, and more. An appropriate first step is drawing a map of the physical facility and identifying the areas and entry points that need different rules of access or levels of security. These areas might have concentric boundaries, such as site perimeter, building perimeter, computer area, computer rooms, and equipment racks. There may also be side-by-side boundaries, such as visitor area, offices, and utility rooms. For concentric boundaries, physical security that provides access control and monitoring at each boundary provides defense in depth. Figure 16.1, from the Schneider Electric white paper *Physical Security in Mission Critical Facilities* [NILE15], depicts such a map.

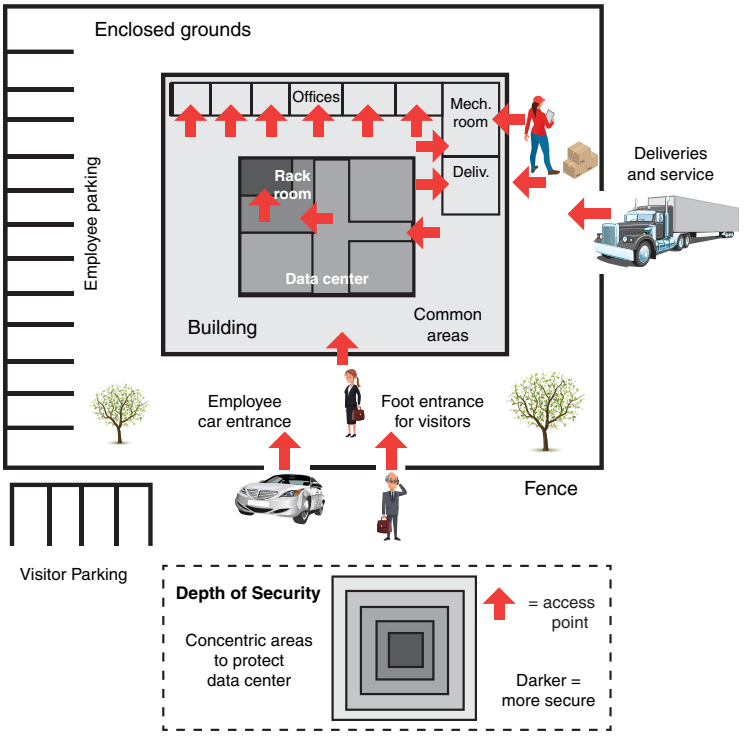


FIGURE 16.1 Security Map Showing Depth of Security

SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*, recommends that authentication mechanisms be selected on the basis of protective areas established around assets or resources. The document adopts the

https://t.me/learningnets

concept of "controlled, limited, and exclusion" areas, as defined in the Department of the Army's *Physical Security* field manual [ARMY10] and summarized in Table 16.2. Procedurally, proof of affiliation is often sufficient to gain access to a controlled area (for example, a company's badge to the outer perimeter of that company's headquarters). Access to limited areas is often based on functional subgroups or roles (for example, a division badge to a particular division's building or wing). The individual membership in the group or privilege of the role is established by authentication of the identity of the cardholder. Access to exclusion areas may be gained by individual authorization only.

TABLE 16.2 Degrees of Security and Control for Protected Areas

Classification	Description
Unrestricted	An area of a facility that has no security interest.
Controlled	The portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled because mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area.
Limited	Restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the security interest. Escorts and other internal restrictions may prevent access within limited areas.
Exclusion	A restricted area containing a security interest. Uncontrolled movement permits direct access to the security interest.

Physical Security: Prevention and Mitigation Measures

This section lists a range of techniques for preventing, or in some cases deterring, physical attacks.

One general prevention measure is the use of cloud computing. From a physical security viewpoint, an obvious benefit of cloud computing is that there is a reduced need for information system assets onsite, and a substantial portion of data assets are not subject to onsite physical threats.

Environmental Threats

The following measures address environmental threats:

- **Natural disasters:** The enterprise needs a natural disaster plan that is coordinated with natural disaster plans of local jurisdictions. At a minimum, the natural disaster plan should provide guidance for the following:
  - Control of operation
  - Evacuation

https://t.me/learningnets

- Communication
- Control of publicity
- Physical security
- An after-action report

Both for site selection and for natural disaster planning, an enterprise needs good information about the level of threat in its location. A good resource for this is the United Nations Office for Disaster Risk Reduction. Another good source is the natural disaster Risk Management Series of publications from the U.S. Department of Homeland Security' Federal Emergency Management Agency (FEMA).



United Nations Office for Disaster Risk Reduction https://www.unisdr.org/we/inform/disaster-statistics

- **Inappropriate temperature/humidity:** Dealing with this problem is primarily a matter of having environmental-control equipment of appropriate capacity and appropriate sensors to warn of thresholds being exceeded. Beyond that, the principal requirement is the maintenance of a power supply.
- **Fire and smoke:** Dealing with fire involves a combination of alarms, preventive measures, and fire mitigation techniques. Table 16.3 summarizes the controls specified in National Institute of Standards and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. To deal with the threat of smoke, the responsible manager should install smoke detectors in every room that contains computer equipment as well as under raised floors and over suspended ceilings. An organization should prohibit smoking in computer rooms. For wildfires, the available countermeasures are limited. Fire-resistant building techniques are costly and difficult to justify.



FEMA Natural Disaster Risk Management Series https://www.fema.gov/security-risk-management-series-publications

TABLE 16.3 Fire Protection Controls

Control	Description
General Fire Protection Guidance	
PE-13	Employ and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.
Fire Protection/Detection Devices and Systems	
PE-13(1)	Employ fire detection devices/systems for the system that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.
Fire Protection/Automatic Suppression Devices and Systems	
PE-13(2)(a)	Employ fire suppression devices/systems for the system that provide automatic notification of any activation to [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined* emergency responders].

https://t.me/learningnets

Control	Description
PE-13(2)(b)	Employ an automatic fire suppression capability for the system when the facility is not staffed on a continuous basis.
Fire Protection/Inspections	
PE-13(4)	Verify that the facility undergoes [*Assignment: organization-defined frequency*] fire protection inspections by authorized and qualified inspectors and resolves identified deficiencies within [*Assignment: organization-defined time-period*].

- **Water:** Prevention and mitigation measures for water threats must encompass the range of such threats. For plumbing leaks, with knowledge of the exact layout of water supply lines, the organization should locate equipment sensibly. It should make sure the location of each shutoff valve is clearly visible or at least clearly documented and that the responsible personnel know the procedures to follow in case of emergency. To deal with both plumbing leaks and other sources of water, sensors are vital. An organization should install water sensors on the floors of computer rooms as well as under raised floors and cut off power automatically in the event of a flood.
- **Chemical, radiological, and biological hazards:** For these threats, an enterprise must employ a range of specific technical approaches, including infrastructure design, sensor design and placement, mitigation procedures, and personnel training. Standards and techniques in these areas continue to evolve.
- **Dust:** An organization should limit dust through proper filter maintenance and regular IT room maintenance.
- **Infestation:** Regular pest control procedures may be needed, starting with maintaining a clean environment.

Technical Threats

The following measures address technical threats:

- **Brief power interruptions:** An organization should use an uninterruptible power supply (UPS) for each piece of critical equipment. A UPS is a battery backup unit that maintains power to processors, monitors, and other equipment for a period of minutes. UPS units also function as surge protectors, power noise filters, and automatic shutdown devices when the battery runs low.
- **Longer blackouts or brownouts:** An organization should connect critical equipment to an emergency power source, such as a generator. For reliable service, management needs to address a range of issues, including product selection, generator placement, personnel training, and testing and maintenance schedules.

https://t.me/learningnets

- **Electromagnetic interference:** An organization should use a combination of filters and shielding. The specific technical details depend on the infrastructure design and the anticipated sources and nature of the interference.

Human-Caused Physical Threats

The following measures address human-caused threats:

- **Unauthorized physical access:** Preventive measures include locks and other hardware, card entry system, and proximity/touch access systems. Deterrence and response measures include intrusion alarms, sensors, and surveillance systems.
- **Theft:** The measures to counter unauthorized physical access apply to the threat of theft as well. In addition, an organization should secure objects from being moved by bolting them down. For movable objects, an organization can incorporate a tracking device and provide an automated barrier that triggers an alarm when tagged objects cross the barrier.
- **Vandalism:** Vandalism may involve environmental threats such as fire or technical threats such as interrupting or surging power, and the corresponding countermeasures apply.

Physical Security Controls

NIST SP 800-53 provides a detailed list of physical and environmental security controls, which are summarized in Table 16.4.

TABLE 16.4 Physical and Environmental Protection Controls

PE-1	**Physical & environmental protection policies & procedures**	PE-9(2)	Automatic voltage controls
PE-2	**Physical access authorization**	PE-10	**Emergency shutoff**
PE-2(1)	Access by position and role	PE-11	**Emergency power**
PE-2(2)	Two forms of identification	PE-11(1)	Long-term alternate power supply—minimal operational capability
PE-2(3)	Restrict unescorted access	PE-11(2)	Long-term alternate power supply—self-contained
PE-3	**Physical access control**	PE-12	**Emergency lighting**
PE-3(1)	System access	PE-12(1)	Essential mission and business functions
PE-3(2)	Facility & system boundaries	PE-13	**Fire protection**

https://t.me/learningnets

PE-3(3)	Continuous guards
PE-3(4)	Lockable casings
PE-3(5)	Tamper protection
PE-3(7)	Physical barriers
PE-4	**Access control for transmission**
PE-5	**Access control for output devices**
PE-5(1)	Access to output by authorized individuals
PE-5(2)	Access to output by individual identity
PE-5(3)	Marking output devices
PE-6	**Monitoring physical access**
PE-6(1)	Intrusion alarms and surveillance equipment
PE-6(2)	Automated intrusion recognition and response
PE-6(3)	Video surveillance
PE-6(4)	Monitoring physical access to systems
PE-8	**Visitor access records**
PE-8(1)	Automated records maintenance & review
PE-9	**Power equipment and cabling**
PE-9(1)	Redundant cabling
PE-13(1)	Detection devices & systems
PE-13(2)	Automatic suppression devices & systems
PE-13(4)	Inspections
PE-14	**Temperature and humidity controls**
PE-14(1)	Automatic controls
PE-14(2)	Monitoring with alarms and notifications
PE-15	**Water damage protection**
PE-15(1)	Automation support
PE-16	**Delivery and removal**
PE-17	**Alternate work site**
PE-18	**Location of system components**
PE-18(1)	Facility site
PE-19	**Information leakage**
PE-19(1)	National emissions and Tempest policies and procedures
PE-20	**Asset monitoring & tracking**
PE-21	**Electromagnetic pulse protection**
PE-22	**Component marking**

As with other controls in SP 800-53, the physical and environmental controls have the following structure:

- A base control section
- A supplemental guidance section
- A control enhancements section
- A related controls section
- A references section

For example, Table 16.3 shows the base control section for fire protection controls. These controls constitute a useful checklist for physical security planning.

https://t.me/learningnets

Control Baselines

SP 800-53 provides a recommended set of minimum security controls, called a *control baseline*, defined for low-impact, moderate-impact, and high-impact systems. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines these categories, which are also described in Chapter 3, "Information Risk Assessment":

- **Low:** Expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
- **Moderate or medium:** Expected to have a serious adverse effect on organizational operations, organizational assets, or individuals
- **High:** Expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

The control baselines are intended to assist an organization in selecting a set of controls for its systems that is commensurate with the risk. A *control baseline* is a collection of controls that address the protection needs of a group, an organization, or a community of interest. The control baseline provides a generalized set of controls that represents an initial starting point for the subsequent tailoring activities that are applied to the baseline to produce a more targeted or customized security and privacy solution for the entity it is intended to serve.

Table 16.5 shows the control baselines defined for the physical and environmental protection controls.

TABLE 16.5 Physical and Environmental Protection Control Baselines

Control		Control Baselines		
		Low	Moderate	High
PE-1	Physical and environmental protection policies and procedures	PE-1	PE-1	PE-1
PE-2	Physical access authorization	PE-2	PE-2	PE-2
PE-3	Physical access control	PE-3	PE-3	PE-3
PE-4	Access control for transmission	—	PE-4	PE-4
PE-5	Access control for output devices	—	PE-5	PE-5
PE-6	Monitoring physical access	PE-6	PE-6(1)	PE-6(1)(4)
PE-8	Visitor access records	PE-8	PE-8	PE-8
PE-9	Power equipment and cabling	—	PE-9	PE-9
PE-10	Emergency shutoff	—	PE-10	PE-10
PE-11	Emergency power	—	PE-11	PE-11(1)
PE-12	Emergency lighting	PE-12	PE-12	PE-12

https://t.me/learningnets

Control		Control Baselines		
		Low	Moderate	High
PE-13	Fire protection	PE-13	PE-13(1)(2)	PE-13(1)(2)
PE-14	Temperature and humidity controls	PE-14	PE-14	PE-14
PE-15	Water damage protection	PE-15	PE-15	PE-15(1)
PE-16	Delivery and removal	PE-16	PE-16	PE-16
PE-17	Alternate work site	—	PE-17	PE-17
PE-18	Location of system components	—	—	PE-18
PE-19	Information leakage	—	—	—
PE-20	Asset monitoring and tracking	—	—	—
PE-22	Electromagnetic pulse protection	—	—	—
PE-23	Component marking	—	—	—

Control Assessment

SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, provides guidance on assessing the effectiveness of security controls and on generating security evidence related to security assessments conducted during the system development life cycle.

For example, Figure 16.2 shows the assessment for fire protection control PE-13(1), listed in Table 16.3.

PE-13(1)	**FIRE PROTECTION | *DETECTION DEVICES / SYSTEMS***	
	ASSESSMENT OBJECTIVE: *Determine if the organization:*	
	PE-13(1)(1)	*defines personnel or roles to be notified in the event of a fire;*
	PE-13(1)(2)	*defines emergency responders to be notified in the event of a fire;*
	PE-13(1)(3)	*employs fire detection devices/systems for the information system that, in the event of a fire:*
	PE-13(1)(3)(a)	*activate automatically;*
	PE-13(1)(3)(b)	*notify organization-defined personnel or roles; and*
	PE-13(1)(3)(c)	*notify organization-defined emergency responders*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service-level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; alerts/notifications of fire events; other relevant documents or records]. Interview: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for notifying appropriate personnel, roles, and emergency responders of fires; organizational personnel with information security responsibilities]. Test: [*SELECT FROM:* Automated mechanisms supporting and/or implementing fire detection devices/systems; activation of fire detection devices/systems (simulated); automated notifications].	

FIGURE 16.2 Control Assessment for Fire Protection Control PE-13(1)

https://t.me/learningnets

The combination of security controls and assessment guidance support an effective physical security policy. In addition, the implementation of these controls and assessment procedures can provide the organization with a degree of protection against various forms of liability.

16.3 Local Environment Management Best Practices

The SGP breaks down the best practices in the local environment management category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Local environments:** This area deals with security issues in end-user environments and other local environments.
  - **Local environment profile:** Covers the items the enterprise should document concerning the type and importance of business conducted in the local environment, including important business and security details about business users, information, technology, and locations.
  - **Local security coordination:** Describes arrangements the enterprise should make to coordinate information security activity in individual business unit departments.
- **Physical and environmental security:** This area deals with the security of critical facilities against targeted cyber attacks, unauthorized physical access, accidental damage, loss of power, fire, and other environmental or natural hazards.
  - **Physical protection:** Lists types of security controls that provide physical protection.
  - **Power supplies:** Discusses recommended approaches to preventing services provided by computer systems from being disrupted by loss of power.
  - **Hazard protection:** Lists security controls for preventing services being disrupted by damage to critical facilities caused by fire, flood, and other types of hazard.

https://t.me/learningnets

16.4 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

defense in depth
environmental threats
human-caused physical threats
information security coordinator
information protection champion
local environment
noise
overvoltage
physical security
physical security officer
security champion
security control
security control baseline
technical threats
undervoltage

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. According to the SGP, what are four key elements of a local environment security profile?
2. What are key responsibilities of a local environment security coordinator?
3. What kind of infrastructure demands a high level of physical security?
4. What are some key environmental threats to physical security?
5. In what ways do electrical power and electromagnetic radiation pose threats to physical security?
6. List and describe some human-caused physical threats.
7. What is the defense in-depth strategy, and how is it applied to physical security?
8. What are some measures that are effective in addressing technical threats?
9. How can an organization counter human-caused physical threats?
10. How does the SGP categorize best practices in the local environment management category?

https://t.me/learningnets

16.5 References

ARMY10: Department of the Army, *Physical Security.* Field Manual FM 3-99.32, August 2010.

ISAC11: ISACA, *Creating a Culture of Security*. 2011. www.isaca.org

NILE15: Niles, S., *Physical Security in Mission Critical Facilities.* White Paper 82. Schneider Electric. March 2015. http://it-resource.schneider-electric.com/h/i/55734850-wp-82-physical-security-in-mission-critical-facilities

https://t.me/learningnets

Chapter 17

Business Continuity

"Well, here's another nice mess you've gotten me into!"

—Stan Laurel

Learning Objectives

After studying this chapter, you should be able to:

- Present an overview of business continuity concepts, including the operation of business continuity management systems, the objectives for business continuity, and the essential components for maintaining business continuity.
- Understand the key elements of a business continuity program.
- Explain the concept of resilience in the context of business continuity.
- Outline the elements of a business continuity plan.
- Discuss performance analysis of a business continuity management system.
- Describe the phases of business continuity operation following a disruptive event.
- Present an overview of business continuity best practices.

A fundamental concern for all organizations is business continuity. An organization needs to perform essential functions during an emergency situation that disrupts normal operations and resume normal operations in a timely manner after the emergency has ended.

The International Organization for Standardization (ISO) has published a family of standards for business continuity management that enterprise security managers should be familiar with:

- **ISO 22300, *Security and Resilience—Vocabulary*:** Provides a glossary of relevant terms.
- **ISO 22301, *Business Continuity Management Systems—Requirements*:** Specifies requirements for setting up and managing an effective business continuity management

https://t.me/learningnets

system (BCMS). This is the first international standard focused exclusively on business continuity.

- **ISO 22313, *Business Continuity Management Systems—Guidance*:** Provides guidance, where appropriate, on the requirements specified in ISO 22301 and provides recommendations ("should") and permissions ("may") in relationship to them.
- **ISO 22317, *Business Continuity Management Systems: Guidelines for Business Impact Analysis (BIA)*:** Provides guidelines (based on good international practice) for performing a business impact analysis (BIA), which is a requirement of ISO 22301 (clause 8.2). It provides guidance for establishing, implementing, and maintaining a formal and documented process for business impact analysis. It is applicable to all organizations, regardless of type, location, size, and nature of the organization.
- **ISO 22318, *Business Continuity Management Systems: Guidelines for Business Impact Analysis (BIA)*:** Provides guidelines for supply chain continuity.

Two additional useful guidance documents are:

- **National Institute of Standards and Technology (NIST) SP 800-34, *Contingency Planning Guide for Federal Information Systems*:** Provides a detailed description of the planning process.
- **European Union Agency for Network and Information Security's (ENISA's) *IT Business Continuity Management: An Approach for Small and Medium Sized Organizations*:** Provides a detailed list of controls for implementing business continuity plans.

Section 17.1 introduces key concepts of business continuity management (BCM). Figure 17.1 provides a useful three-layer model for BCM, covering governance and policy, readiness, and operations. Sections 17.2 through 17.4 address these areas in turn.

Figure 17.2 provides another view of BCM, showing the flow between the major elements, as suggested in ISO 22301.

BCM is a broad area that deals with all sorts of disasters, including natural disasters, health and safety incidents, and cyber attacks. ISO 27002, *Code of Practice for Information Security Controls*, specifically focuses on threats to information assets and information and communications technology (ICT) systems. This chapter describes BCM in general terms, with specific reference to information assets and ICT systems, where appropriate.

https://t.me/learningnets

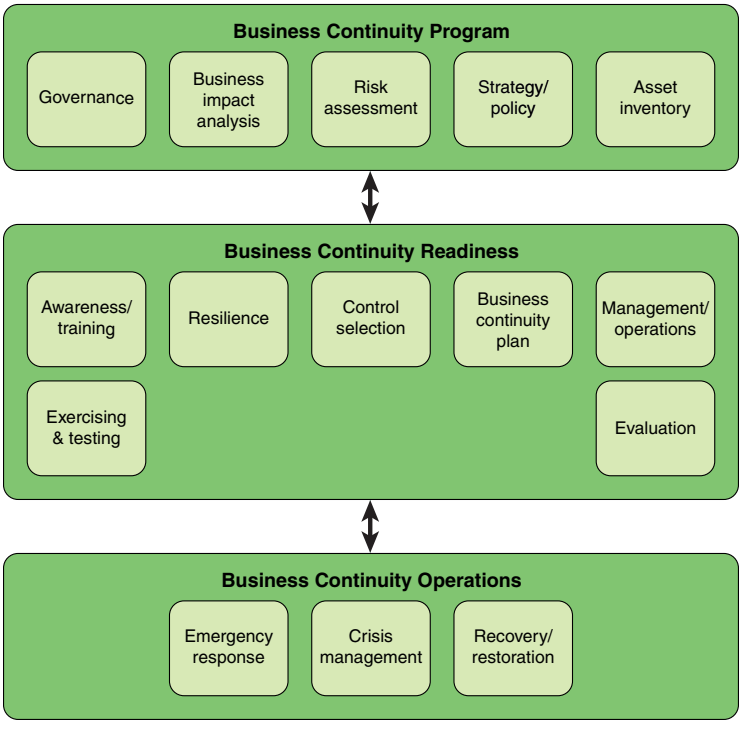


FIGURE 17.1 Elements of Business Continuity Management

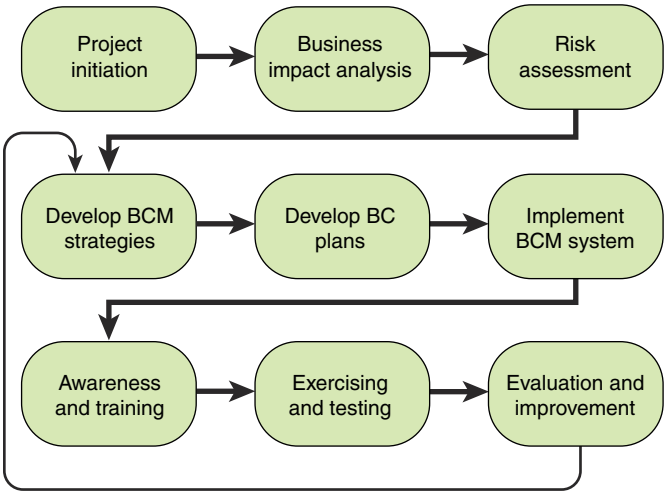


FIGURE 17.2 ISO 22301 Methodology for BCM

https://t.me/learningnets

17.1 Business Continuity Concepts

This section provides an overview of business continuity. After providing a number of important definitions, the section surveys threats to business continuity and a general look the typical enterprise approach to business continuity. The following definitions, based on those in ISO 22300, are relevant for the discussion in this chapter:

- **Business:** For purposes of discussing business continuity, the operations and services performed by an organization in pursuit of its objectives, goals, or mission. As such, it is equally applicable to large, medium, and small organizations operating in industrial, commercial, public, and not-for-profit sectors.
- **Business continuity:** The capability of an organization to continue delivering products or services at acceptable predefined levels following a disruptive incident. Business continuity embraces all the operations in a company, including how employees function in compromised situations.
- **Business continuity management (BCM):** A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and that provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.
- **Business continuity management system (BCMS):** Part of an overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity. The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes, and resources.
- **Business continuity manager:** An individual who manages, designs, oversees, and/or assesses an enterprise's business continuity capability to ensure that the enterprise's critical functions continue to operate following disruptive events.
- **Business continuity plan (BCP):** The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
- **Business continuity program:** An ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

https://t.me/learningnets

Threats

It should be clear that a high priority for every organization is the ability to prevent, if possible, and recover rapidly, if necessary, from a substantial disruption of operations and/or resource availability. The importance of planning for business continuity is evident when considering the broad range of threats to continuity. These threats can be grouped as natural disasters, systems problems, cyber attacks, and human-caused disasters. The following list is based on threats defined in *ENISA IT Business Continuity Management: An Approach for Small and Medium Sized Organizations* [ENIS10] and the Federal Financial Institutions Examination Council's *Business Continuity Planning* [FFIE15].

Natural Disasters

Threats in the natural disaster category include the following:

- **Accidental fire:** Sources include wildfires, lightning, wastebasket fires, and short-circuits.
- **Severe natural event:** This category includes damage resulting from an earthquake, a hurricane, a tornado, or other severe weather, such as extreme heat, cold, humidity, wind, or drought.
- **Accidental flood:** Causes of flooding include pipe leakage from air-conditioning equipment, leakage from a water room on the floor above, fire nozzle being open, accidental triggering of sprinkler systems, broken water main, and open window during a rainstorm.
- **Accidental failure of air conditioning:** Failure, shutdown, or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction, or fail completely.
- **Electromagnetic radiation:** Electromagnetic radiation originates from an internal or external device, such as radar, radio antenna, and electricity-generating station. It can interfere with proper functioning of equipment or quality of service of wireless transmission and reception.
- **Air contaminants:** Some disasters produce a secondary problem by polluting the air for a wide geographic area. Natural disasters such as flooding can also result in significant mold or other contamination after the water has receded. Nearby discharge or release of hazardous materials may also produce an airborne threat. The severity of these contaminants can affect air quality at an institution and may even result in evacuation for an extended period of time (for example, in the case of volcanic eruptions).

https://t.me/learningnets

Systems Problems

Systems problems include the following:

- **Software malfunction:** A design error, an installation error, or an operating error committed during modification can cause incorrect execution.
- **Equipment malfunction/failure:** Threats include a logical or physical event causing an equipment item to malfunction and/or problem due to failure to follow equipment qualification procedures after updates/upgrades or use of equipment under conditions outside its operating limits (such as temperature or humidity).
- **Breach of information system maintainability:** Lack of expertise in the system may make retrofitting and upgrading impossible. Examples are inability to correct an operating problem or respond to new needs, failure of external software and hardware maintenance companies, and termination of a support contract leaving a lack of competency or resources for system upgrades.

Cyber Attacks

Chapter 14, "Technical Security Management," discusses the numerous technical threats to ICT systems, and Chapter 15, "Threat and Incident Management," discusses cyber attacks in some detail, again with a focus on ICT systems.

With reference to the broader issue of business continuity, management must also be aware of threats to cyber-physical systems. NIST SP 1500-201, *Framework for Cyber-Physical Systems: Volume 1, Overview*, defines a *cyber-physical device* as a device that has an element of computation and interacts with the physical world through sensing and actuation. It defines a *cyber-physical system* (*CPS*) as a smart system that includes engineered interacting networks of physical and computational components. CPS generally involve sensing, computation, and actuation. CPS involve traditional information technology (IT), as in the passage of data from sensors to the processing of those data in computation. CPS also involves traditional operational technology (OT) for control aspects and actuation. The combination of these IT and OT worlds along with associated timing constraints is a particularly new feature of CPS. As organizations rely on CPS, such as in the area of CPS, they need to consider a range of threats to both the IT and OT aspects of CPS. A discussion of this complex area is beyond the scope of this book; see NIST SP 1500-202, *Framework for Cyber-Physical Systems: Volume21, Working Group Reports*, for details.

Human-Caused Disasters

Human-caused threats include the following:

- Theft of equipment
- Deliberate fire

https://t.me/learningnets

- Deliberate flood
- Deliberate loss of power supply
- Deliberate failure of air conditioning
- Destruction of equipment or media
- Unauthorized use of equipment
- Vandalism and explosive discharges

Business Continuity in Operation

In essence, business continuity management is concerned with mitigating the effects of disasters. Figure 17.3, based on figures in ISO 22313, illustrates the two ways in which business continuity management achieves that mitigation. The relative distances depicted in the figure imply no specific time scales. The gray curve shows the pace of recovery from a disaster with a business continuity plan in place, and the black curve shows the typical recovery pace without a business continuity plan.

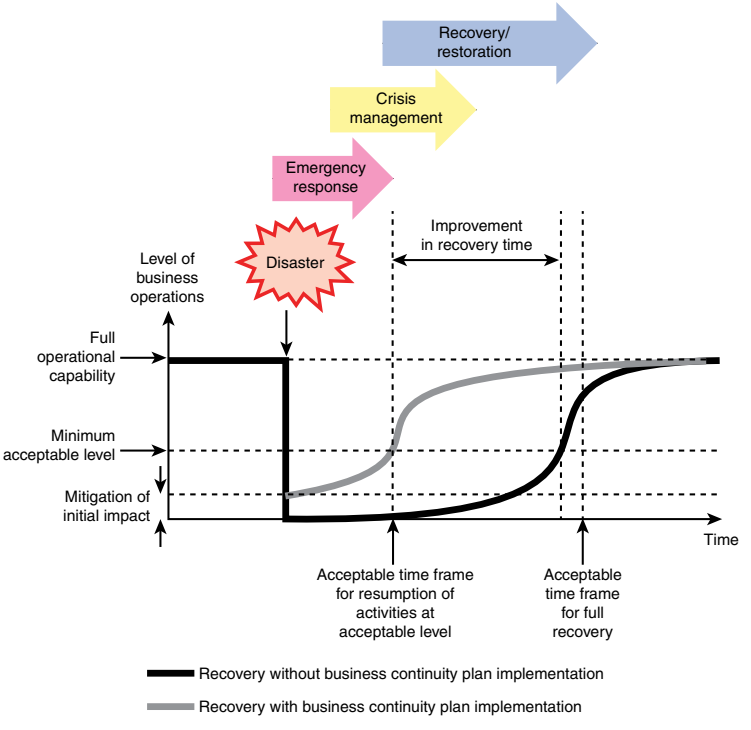


FIGURE 17.3 Effectiveness of Business Continuity Management

https://t.me/learningnets

When a disaster occurs, the worst-case scenario is that it has the potential to bring some business processes or functions to a complete halt. A business continuity plan includes resilience properties and quick or instantaneous switchover mechanisms that mitigate this initial impact. A business continuity plan also calls for the implementation of capabilities and procedures that result in more rapid restoration of operational capability.

Figure 17.3 also depicts that the recovery process goes through three overlapping stages. Section 17.4 discusses this process.

Business Continuity Objectives

Enterprises undertake business continuity planning to reduce the consequences of any disruptive event to a manageable level. The specific objectives of a particular organization's continuity plan may vary, depending on its mission and functions, its capabilities, and its overall continuity strategy. The Federal Emergency Management Agency's *Continuity Guidance for Non-Federal Entities* [FEMA09] outlines the following objectives for business continuity management:

- Minimize loss of life, injury, and property damage.
- Mitigate the duration, severity, or pervasiveness of disruptions that do occur.
- Achieve timely and orderly resumption of essential functions and the return to normal operations.
- Protect essential facilities, equipment, records, and assets.
- Be executable with or without warning.
- Meet the operational requirements of the respective organization. Continuity plans may need to be operational within minutes of activation, depending on the essential function or service, but certainly should be operational no later than 12 hours after activation.
- Meet the sustainment needs of the respective organization. An organization may need to plan for sustained continuity operations for up to 30 days or longer, depending on resources, support relationships, and the respective continuity strategy adopted.
- Ensure the continuous performance of essential functions that require additional considerations beyond traditional continuity planning (such as pandemic influenza).
- Provide an integrated and coordinated continuity framework that takes into consideration other relevant organizational, governmental, and private-sector continuity plans and procedures.

https://t.me/learningnets

Essential Components for Maintaining Business Continuity

An organization's resilience is directly related to the effectiveness of its business continuity capability. An organization's continuity capability rests on the following key components that are essential to maintaining business continuity:

- **Management:** Continuity of management is critical to ensure continuity of essential functions. An organization should have a detailed contingency plan that indicates a clear line of succession so that designated backup individuals have the authority needed to maintain continuity when key managers are unavailable.
- **Staff:** There is a twofold requirement with respect to staff. First, all staff should be trained on how to maintain **continuity of operations (COOP)** or restore operations in response to an unexpected disruption. Second, the organization should develop guidelines for vertical training and cross training so that staff can take on functions of peers and those above and below them in the reporting hierarchy, as needed.
- **ICT systems:** A top priority following a disruption is communications, both internal and external. Communication systems and technology should be interoperable, robust, and reliable. An organization should identify critical IT systems and have backup and rollover capabilities tested and in place
- **Buildings and equipment:** This component includes the buildings where essential functions are performed. Organizations should have separate backup locations available where management and business process functions can continue during disruptions that in some way disable the primary facility. This component also covers essential equipment and utilities.

continuity of operations (COOP)

An effort in an organization to ensure that it can continue to perform the essential business functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

17.2 Business Continuity Program

Recall from Chapter 2, "Security Governance," that an information security program consists of the management, operational, and technical aspects of protecting information and information systems. It encompasses policies, procedures, and management structure and mechanism for coordinating security activity. A business continuity program, as defined in the beginning of this chapter, encompasses these considerations, although it is not limited to just ICT systems but covers the broader business continuity area.

https://t.me/learningnets

Governance

Business continuity governance is concerned with establishing and maintaining management structures and processes that provide a framework for maintaining business continuity in response to major security incidents and disasters.

A typical process for establishing the management framework includes the following tasks:

- Executive management meets to define objectives and goals of a business continuity strategy and policy.
- Senior management appoints a business continuity director and a BCM steering committee.
- Business continuity specialists prepare a business/process effort chart, showing level of effort and time, as well as a project plan. Key items include:
  - Identifying key/critical services
  - Determining exclusions from the BCM scope
  - Determining implementation timeline goals
- Executive management communicates to all directors and managers about the upcoming business continuity planning program.
- Department heads commit to goals of business continuity planning.
- Department directors and managers appoint point-of-contact individuals.
- The business continuity director meets with department directors and managers to discuss objectives.

Business Impact Analysis

SP 800-34 defines *business impact analysis* (*BIA*) as analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. A BIA helps identify and prioritize information systems and components that are critical to supporting the organization's mission/business processes.

A typical BIA includes the following steps:

1. Inventory key business elements, including:
   - Business processes
   - Information systems/applications

https://t.me/learningnets

- Assets
- Personnel
- Suppliers

2. Develop intake forms to gather consistent information, interview key experts throughout the business, and get information from inventories.
3. Assess and prioritize all business functions and processes, including their interdependencies.
4. Identify the potential impact of business disruptions resulting from uncontrolled, nonspecific events on the institution's business functions and processes.
5. Identify the legal and regulatory requirements for the institution's business functions and processes.
6. Determine the **maximum tolerable downtime (MTD)** for each business process.
7. Calculate a reasonable **recovery time objective (RTO)** and **recovery point objective (RPO)** for each business process. The processes with the shortest MTD or RTO are the most critical business processes. Get agreement from senior management.

maximum tolerable downtime (MTD)
The amount of time after which an organization's viability is irrevocably threatened if product and service delivery are not resumed.

recovery time objective (RTO)
The target time set for resumption of product, service, or activity delivery after an incident. It is the maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions must be recovered after an outage (for example, the point in time at which a process can no longer be inoperable).

recovery point objective (RPO)
The amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (for example, the date and time of a business disruption).

The result of a BIA is to identify time-sensitive processes and the requirements to recover them in the time frame that is acceptable to the entity.

Risk Assessment

An organization needs to perform a risk analysis on each critical process to identify any vulnerabilities that exist, along with steps to mitigate those vulnerabilities. Chapter 3, "Information Risk Assessment," discusses this process in detail for security management, and the same process applies for business continuity.

In essence, business continuity risk assessment addresses three questions: What can go wrong? What is the likelihood that the undesired event might occur? and What would be the impact should it occur? FEMA's *Continuity Guidance for Non-Federal Entities* [FEMA09] defines the following critical steps in the risk assessment process:

1. **Inventory the essential functions provided by the organization.** These are the functions whose interruption causes unacceptable business impact.
2. **Identify the threats that can impact delivery of the essential functions.** This step includes exploring potential natural events, systems events, intentional

https://t.me/learningnets

human events, and non-intentional human-caused events that could adversely affect the ability of the organization to perform its essential functions.

3. **Develop continuity hazard scenarios.** Perform all of these assessment steps within the context of a set of scenarios, each of which is a unique combination of a particular hazard and the organization's essential functions. Within each scenario, consider risks to the four key elements management, staff, ICT systems, and facilities, as appropriate. Scenario risk assessment includes the following steps:
    a. **Determine the risk information needed to assess the risk.** Describe the information necessary to assess the risk for each scenario. For each information item, specify the information type, precision, and certainty required, as well as the analysis resources available.
    b. **Assess the risk.** For each scenario, assess the threat, vulnerability, and consequence, where:
        - Threat is the likelihood of a type of attack that might be attempted or that the scenario will occur.
        - Vulnerability is the likelihood that an attacker would succeed with a particular attack type or that the scenario will result in the expected level of consequence.
        - Consequence is the potential impact of a particular attack or the negative impact of the scenario.
4. **Identify existing safeguards/countermeasures.** For each scenario, identify the existing safeguards that are in place to reduce either the likelihood (for example, security countermeasures) or consequence (for example, redundant capabilities) of the hazard.

Table 17.1, from *ENISA IT Business Continuity Management: An Approach for Small and Medium Sized Organizations* [ENIS10], provides a set of categories that an assessment team can use to evaluate the organization's risk profile.

TABLE 17.1 Risk Profile Evaluation Table

Risk Area	High	Medium	Low
Legal and Regulatory			
Sensitive/personal customer data	Handles sensitive/ personal customer data	Handles personal customer data	Does not handle personal customer data
Loss/destruction of such data	Will lead to significant legal fines	Will lead to legal fines	N/A

https://t.me/learningnets

Risk Area	High	Medium	Low
Failure to meet agreed service level agreements (SLAs) with customers	Will result in non-frivolous lawsuits	May result in non-frivolous lawsuits	N/A
Productivity			
Services and operational processes	Highly dependent on information systems, applications, and third-party services	Dependent on information systems, applications, and third-party services	Not directly dependent on information systems, applications, and third-party services
Interruptions to the provision of the aforementioned	Requires significant expenses and effort to resume business and recover from market loss	Organization can use backup procedures for a limited time without significant productivity effect	Organization can use backup procedures for a time without productivity effect
Financial Stability			
Unavailability of products of less than one day	Major one-time financial loss	Significant one-time financial loss	No financial loss
Revenues related to continuous provision of online services	Directly	Indirectly	Not related
Unavailability of online presence	Will lead to direct financial loss	Will not lead to direct financial loss	Will not lead to direct or indirect loss
Fines due to noncompliance with legal and regulatory requirements	May lead to intolerable financial loss	Possible but will not affect financial stability	No or marginal fines
Reputation and Loss of Customer Confidence			
Unavailability of service	Significant loss of customers	Considerable loss of customers	Marginally noticed by customers

Business Continuity Strategy

A business continuity strategy is a conceptual summary of preventive and recovery strategies that must be carried out between the occurrence of a disaster and the time when normal operations are restored. Strategy design involves understanding the requirements gathered during the business impact analysis and risk assessment and effectively translating them into actionable strategies. Furthermore, it involves considering the costs/benefits of any proposed strategy.

https://t.me/learningnets

Figure 17.4 illustrates the type of trade-off that management needs to consider. The cost of disruption derives from the business impact analysis and risk assessment. Against that is the cost of resources to implement a business continuity program. Typically, the longer a disruption continues, the more costly it becomes for the organization. But the shorter the RTO, the more costs are incurred. For example, for short recovery times, an organization may require a mirror data site that is always active and updated, whereas a longer RTO may enable the enterprise to rely on a less costly tape backup system.

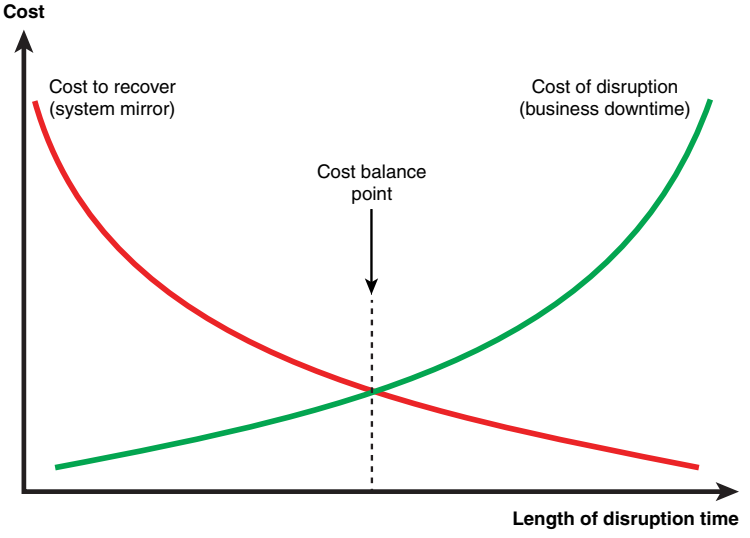


FIGURE 17.4 Cost Balancing for Business Continuity Management

The business continuity strategy does not indicate specific security controls; that is the task of the business continuity plan. Rather, the business continuity strategy is at a higher, strategic, level and provides overall guidance.

ISO 22301 divides business continuity strategy into three categories: determination and selection, resource requirements, and protection and mitigation.

Determination and Selection

The first category of developing a business continuity strategy, and the first part of a business continuity document, consists of determining possible business continuity strategies based on the business impact analysis and risk assessment.

ISO 22301 calls out three areas to be considered in developing the strategy:

- **Protecting prioritized activities:** For activities deemed significant for maintaining continuity, the organization needs to look at the general strategic question of how each activity is carried out. The goal is to determine a strategy that

https://t.me/learningnets

reduces the risk to the activity. The organization should also consider alternatives, including outsourcing (for example, using cloud services) or fundamentally altering the activity to avoid risk.

- **Stabilizing, continuing, resuming, and recovering prioritized activities and their dependencies and supporting resources:** The organization should provide more detailed options for managing each prioritized activity during the business continuity process. Examples include:
  - Temporarily relocating an activity to a backup site or relocating some for the IT and other resources that support the activity
  - Using redundant equipment and other resources during the business continuity process
  - Making substitutions for the normal activity that may involve different personnel, different resources, and/or different processes
- **Mitigating and responding to impacts:** Finally, the organization should spell out its strategies for containing the damage to the organization from disasters. These strategies may include insurance, preplanned replacement/repair service, and a plan for maintaining the company's reputation.

Resource Requirements

The purpose of the resource requirements category is to determine the resources necessary to implement each of the business continuity strategy categories. ISO 22301 lists the following types of resources to consider:

- **People:** Consider a number of questions, such as the following:
  - Does there need to be one or more dedicated business continuity officers?
  - What level of effort is required of other employees to participate in business continuity implementation and the business continuity process?
  - What resource commitment is needed for awareness programs and training?
- **Information and data:** Estimate the resources needed to maintain backup and redundant copies of critical information assets.
- **Buildings, work environment, and associated utilities:** Include the cost of hardening or protecting resources as well as the cost of any standby or fallback facilities that the organization maintains.
- **Facilities, equipment, and consumables:** Include estimates for protecting and providing redundancy.
- **ICT systems:** Estimate resources for protecting and providing redundancy for ICT systems.

https://t.me/learningnets

- **Transportation:** Consider the possibility of moving equipment and personnel for the duration of the response and recovery phase.
- **Finance:** Determine options to ensure needed financing for the duration of an incident to meet extra expenses associated with response and recovery.
- **Partners and suppliers:** Indicate what commitments are needed from partners and suppliers and what the cost to the organization will be.

Protection and Mitigation

Both ISO 22301 and 22313 refer to protection and mitigation as part of developing a strategy. This category is best viewed as the culmination of developing a strategy, when those involved in developing the business continuity strategy submit the strategy options and recommendations to management for feedback, selection, and approval. With the information provided, management can evaluate the cost/benefit analysis to determine the optimal strategies, based on requirements and the organization's risk appetite.

17.3 Business Continuity Readiness

Business continuity readiness, refers to the capability of an organization and its assets to respond to, manage, and recover from a disruptive event. This section looks at the actions taken to prepare for such disruptive and disastrous events.

Awareness

An awareness program ensures that an organization's personnel are aware of the importance of business continuity and understand their roles in maintaining business continuity. An organization should ensure that all staff learn about awareness as part of the induction program for new hires and then an ongoing basis. The objectives of an awareness program include:

- Establishing objectives of a BCM awareness and training program
- Identifying functional awareness and training requirements
- Recognizing appropriate internal and external audiences
- Developing awareness and training methodology
- Identifying, acquiring, or developing awareness tools
- Leveraging external awareness opportunities
- Overseeing the delivery of awareness activities
- Establishing the foundation for evaluating the program's effectiveness

https://t.me/learningnets

- Communicating implications of not conforming to BCM program requirements
- Ensuring continual improvement of the BCM program
- Confirming that personnel are aware of their roles and responsibilities in the BCM program

An awareness session should cover the following topics:

- An overview of what BCM is
- Why BCM is important to the organization
- The staff's role in an emergency
- What staff should do if the BCM plan is invoked
- The emergency contact numbers
- Identification and escalation of incidents
- Triggers for incident response and activation of the business continuity plan(s)
- How to respond to special events
- Measures to be taken during site evacuation

Training

Training provides skills and familiarizes leadership and staff with the procedures and tasks to perform in executing continuity plans. FEMA's *Continuity Guidance for Non-Federal Entities* [FEMA09] recommends that a training program include the following:

- Annual training for personnel (including host or contractor personnel) who are assigned to activate, support, and sustain continuity operations
- Annual training for the organization's leadership on that organization's essential functions, including training on individual position responsibilities
- Annual training for all organization personnel who assume the authority and responsibility of the organization's leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity situation
- Annual training for all pre-delegated authorities for making policy determinations and other decisions, at the field, satellite, and other organizational levels, as appropriate
- Personnel briefings on organization continuity plans that involve using or relocating to continuity facilities, existing facilities, or virtual offices

https://t.me/learningnets

- Annual training on the capabilities of communications and IT systems to be used during an incident
- Annual training regarding identification, protection, and availability of electronic and hard copy documents, references, records, information systems, and data management software and equipment (including sensitive data) needed to support essential functions during a continuity situation
- Annual training on an organization's devolution option for continuity to address how each organization identifies and conducts its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency
- Annual training for all reconstitution plans and procedures to resume normal organization operations from the original or replacement primary operating facility

In terms of the specific content of training, the National Emergency Crisis and Disasters Management Authority's *Business Continuity Management Standard and Guide* [NCEM12] recommends the following:

- Include procedures for evacuation, shelter-in-place, check-in at the evacuation site, responsibility toward employees, activation and preparation of alternative work sites, and handling of requests for information by internal and external stakeholders
- Provide response and recovery teams education and training on their responsibilities and duties, including how to interact with first responders

Resilience

Resilience of the infrastructure, assets, and procedures of an enterprise—referred to as **information system resilience**—improves the organization's ability to withstand and recover from disruptive events.

The IBM white paper *Resilient Infrastructure: Improving Your Business Resilience* [GOBL02] defines elements of **business resilience**. The first three are primarily defensive in nature but are the common strategies used by enterprises and a necessary part of business continuity management:

- **Recovery:** The provision for safe, rapid, offsite data recovery in the event of a disaster
- **Hardening:** The fortification of all or part of an infrastructure to make it less susceptible to natural disaster, employee error, or malicious actions
- **Redundancy:** The duplication of all or part of the infrastructure to supply hot, active backup service in the event of an unanticipated event

information system resilience

The ability of an information system to continue to (1) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and (2) recover to an effective operational posture in a time frame consistent with mission needs.

business resilience

The ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and overall brand equity. Business resilience goes a step beyond disaster recovery, offering post-disaster strategies to avoid costly downtime, shore up vulnerabilities, and maintain business operations in the face of additional, unexpected breaches.

https://t.me/learningnets

Resilient Infrastructure: Improving Your Business Resilience [GOBL02] also defines three offensive measures that go beyond traditional approaches to resilience:

- **Accessibility:** If the primary work site is inaccessible, accessibility measures enable enterprise personnel, partners, and customers to access the infrastructure from other locations. These measures include the deployment of diverse communication technologies (for example, wireless, fax, email, instant messaging).
- **Diversification:** In order to decrease the probability that a single disaster will significantly degrade business operations, diversification measures entail the physical distribution of resources (hard assets and people) and implementation of diverse communication pathways. These measures should create an operational infrastructure that is physically distributed but capable of being managed as if it were a single consolidated entity.
- **Autonomation:** This refers to the inclusion of self-managed hardware and software components in the infrastructure. These products make decisions without human intervention or, at a minimum, bypass a problem and alert a human attendant to initiate appropriate action. Many such products are available today, and more will be introduced in the near future. As technology progresses, resilient infrastructures will contain more autonomic components with self-configuring, self-healing, self-protecting, and self-optimizing capabilities.

Control Selection

Control selection, as discussed in other chapters, is the selection of specific measures related to assets and operations that meet the security objective. *ENISA IT Business Continuity Management: An Approach for Small and Medium Sized Organizations* [ENIS10] provides a comprehensive set of controls in two categories: organizational continuity controls and asset-based continuity controls. There are 5 sets of organizational continuity controls, each containing a number of specific controls, for a total of 39 controls. These are the categories:

- **Business continuity management:** Includes controls that require the organization's business strategies to routinely incorporate business continuity considerations
- **Business continuity policy, plans, and procedures:** Requires an organization to have a comprehensive set of documented, current business continuity policies, plans, and procedures that are periodically reviewed and updated
- **Test business continuity plan:** Incorporates security controls in order to complete a test simulation of the continuity plan to ensure its smooth running if the time comes to implement it

https://t.me/learningnets

- **Sustain business continuity management:** Includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel
- **Service providers/third parties business continuity management:** Includes security controls that enforce documented, monitored, and enforced procedures for protecting the organization's information when working with external organizations

The following is an example of a control in the *business continuity policy, plans, and procedures* category:

> The organization has a comprehensive business continuity plan, which is periodically reviewed and updated. The plan address key business continuity topic areas, including:
>
> - Critical Business Functions Priority List
> - Critical Business Functions IT Infrastructure Dependencies
> - Contact List(s) with Business Continuity Manager/Team
> - Critical Business Functions Protection & Recovery Strategy
> - Business Continuity Relative Procedures (Incident Response, Emergency, etc.)
> - Testing Reassessing and Maintaining Business Continuity Plan
> - Critical Suppliers List & Contact Details

The asset-based continuity controls are more extensive and comprise 92 controls in 5 sets:

- **Hardware and network:** Covers resilience, backup, redundancy, and recovery actions
- **Application:** Covers resilience, backup, and recovery actions
- **Data:** Covers data storage, data backup, and recovery actions
- **People:** Covers physical security, awareness and training, and recovery actions
- **Facilities:** Covers IT site, environmental security, physical security, and recovery actions

The following is an example of a control in the application category:

> **Application Backup:** Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and

https://t.me/learningnets

verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules. When this control is applied to a service (such as email or internet provisioning) then establishing an alternate backup service is required in addition to backing up any relevant data. When considering backup of services that produce or store data the ability to have a usable local copy of the data or to transfer existing data to the backup service has to be considered and evaluated.

An organization should use the business impact analysis and the risk assessments as inputs to a selection process for determining the cost/benefit of each control in order to make an optimal selection.

Business Continuity Plan

Whereas a *business continuity strategy* provides an overall view of an enterprise's approach to business continuity management, a *business continuity plan* establishes documented procedures and resources for preparing for and responding to disruptive incidents.

ISO 22301 requires that an organization produce a business continuity plan or an interrelated set of business continuity plans. The organization should establish documented procedures for responding to a disruptive incident and identify how it will continue or recover its activities within a predetermined time frame. The plan or plans should address the requirements of the plan(s) users. ISO 22313 provides guidelines on the development of the plan or plans.

There is no single approach that all organizations can use to develop and document business continuity procedures. The end goal is to create a response structure, warning and communication procedures, and recovery plans that result in a repeatable, effective response and recovery process that can be invoked and executed without delay following the onset of a disruptive incident.

The Western Australian Government's *Business Continuity Management Guidelines* [WAG15] provides useful guidance on the content of a set of plans that covers all phases of business continuity operations, consisting of an overview document, an emergency response plan, a crisis management plan, and a set of recovery and restoration plans (see Figure 17.5). The following sections provide plan outlines from *Business Continuity Management Guidelines*.

https://t.me/learningnets

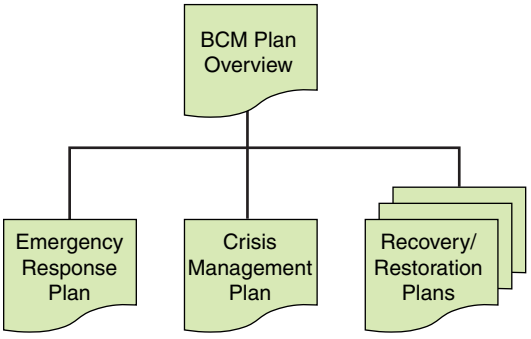


FIGURE 17.5 Components of BCM Plan Documentation

BCM Plan Overview

A BCM plan overview is a description of the framework, policy, processes, and overall strategies for providing for business continuity readiness and performing business continuity operations. The overview document does not provide specific guidance on dealing with disruptions. Rather, it documents the organization's approach to business continuity.

As an example, per *Business Continuity Management Guidelines* [WAG15], a BCM plan overview document may contain the following sections:

1. Version Control Information
2. Distribution List
3. Purpose of the BCM Plan
4. Objectives of the BCM Plan
5. BCM Policy
6. BCM Process Overview
7. Critical Business Activities
   a. Maximum Acceptable Outage
   b. Interdependencies
8. Business Continuity Strategies and Requirements
   a. Broad Strategies
   b. Resource Requirements
   c. Systems and Applications Requirements
9. Response Options
   a. Planning Parameters
   b. Business Continuity Site

https://t.me/learningnets

10. Response Plan
    a. Guiding Principles
    b. Crisis Management Organization
        i. Crisis Management Team
        ii. On Scene Response Team
        iii. Crisis Support Teams
        iv. Business Continuity Teams
        v. IT Disaster Recovery Team
    c. Notification and Escalation Process
    d. Command Centre
11. Training, Exercise and Maintenance
    a. Training Requirements and Protocols
    b. Exercise Requirements and Protocols
    c. Maintenance Requirements and Protocols

Emergency Response Plan

An emergency response plan covers actions that should take place immediately following a critical incident for the protection of people and assets.

According to *Business Continuity Management Guidelines* [WAG15], an emergency response plan document may contain the following sections:

1. Introduction
    1.1. Definitions
    1.2. Purpose
2. Emergency Reporting Procedures
    2.1. Basic Reporting Procedures
    2.2. Priorities of Directive
    2.3. Emergency Telephone Numbers
3. Prevention
    3.1. Fire Prevention
    3.2. Accident Prevention
4. First Aid
5. Responding to Emergencies
    5.1. Fire Emergency
    5.2. Earthquake Emergency

https://t.me/learningnets

5.3. Bomb Threats

5.4. Robberies and Hold-ups

5.5. Kidnapping – Hostage Situation

Crisis Management Plan

A crisis management plan provides guidance on dealing with disruptive incidents after the initial emergency response. Such a plan should provide guidance on quickly developing an organized, systematic response that seeks to maintain some level of continuity.

A crisis management plan document may contain the following eight sections [WAG15]:

1. Purpose
   1.1. Outlines the purpose of the plan and circumstances under which the plan is to be used
2. Definition of Crisis Events
   2.1. Defines what constitutes a crisis event that leads to the activation of the Crisis Management Plan
3. Crisis Management Team Structure
   3.1. Outlines the purpose and membership of the Crisis Management Team
   3.2. Describes the roles and responsibilities of the team members
4. Notification and Escalation Process
   4.1. Outlines the process by which an incident is reported, assessed, and escalated through various levels of management, leading to the activation of the Crisis Management Team
5. Command Centre
   5.1. Describes the purpose of the command center, its location and resources to be made available to support the Crisis Management Team
6. Communications During a Crisis
   6.1. Describes the communications protocols and tools to be used, how events are to be tracked and recorded and how status updates are to be communicated in a crisis situation
7. Contact Lists
   7.1. Contact lists of the Crisis Management Team members, senior management, key staff, service providers, emergency services and other stakeholders who need to be informed and/or are needed to provided assistance during a crisis situation

https://t.me/learningnets

8. Actions Checklists
    8.1. Checklists of issues and actions that the Crisis Management Team need to consider for crisis management response and business continuity. These serve as reminders to ensure that no critical issues or actions are forgotten in the confusion and chaos that may result in a crisis situation.

Recovery/Restoration Plans

Recovery/restoration plans are targeted at individual teams that are responsible for responding to certain types of disruption or supporting certain aspects of recovery and restoration. The objective is to define the procedures and needed resources for maintaining critical business activities and for recovering as quickly as possible in order to resume normal operations.

A recovery/restoration plan document may contain the following sections [WAG15]:

1. Purpose
2. Team Charter
3. Team Composition
4. Activities and Strategy
5. Phase 1: Assessment and Notification
    5.1. Incidents during office hours
        i. Initial Alert
        ii. Evacuation
        iii. Initial Assessment
        iv. Plan Invocation
    5.2. Incidents outside office hours
        i. Initial Alert
        ii. Initial Assessment
        iii. Plan Invocation
6. Phase 2: Plan Activation
    6.1. Upon arrival at business continuity site
    6.2. Business resumption
        i. Within 1 day
        ii. Within 3 days
        iii. Within 5 days
        iv. Within 10 days

https://t.me/learningnets

7. Phase 3: Return to Normalcy
   7.1. Damage assessment
   7.2. Salvage and restoration
   7.3. Relocation

Appendix 1 Contact Lists

Appendix 2 Resource Requirements

Appendix 3 System/Application Requirements

Appendix 4 Vital Records Requirements

Exercising and Testing

Exercising and testing are essential for an organization to validate its ability to effectively respond to and recover from disruptive incidents in the time frame established by management. Exercising and testing must be ongoing to accommodate staff turnover as well as changes in facilities, equipment, and the threat environment.

ISO 22300 defines the terms *exercise* and *test* as follows:

- **Exercise:** A process to train for, assess, practice, and improve performance in an organization. Exercises can be used for:
  - Validating policies, plans, procedures, training, equipment, and interorganizational agreements
  - Clarifying and training personnel in roles and responsibilities
  - Improving interorganizational coordination and communications
  - Identifying gaps in resources
  - Improving individual performance
  - Identifying opportunities for improvement and controlled opportunity to practice improvisation
- **Test:** A procedure for evaluation; a means of determining the presence, quality, or veracity of something.
  - A *test* may be referred to as a *trial*.
  - Testing is often applied to supporting plans.
  - A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

https://t.me/learningnets

An exercise focuses on the business continuity plan and tries to determine if the personnel, procedures, and equipment are all in place and in a state of readiness to respond to an incident. Testing focuses more on individual aspects of business continuity and ensures that equipment and procedures are maintained in a constant state of readiness to support continuity activation and operations.

Exercises

Exercises are needed to assure the organization that its business continuity procedures are reliable. Even for well-designed and analyzed procedures, exercises suggest areas for improvement and often uncover flaws in procedures.

The following is a list, in increasing order of complexity, of types of exercises:

- **Seminar exercise (or plan walkthrough):** An exercise in which the participants are divided into groups to discuss specific issues.
- **Tabletop exercise:** A facilitated exercise in which participants are given specific roles to perform, either as individuals or groups. This book's document resource site provides an example of a business continuity tabletop exercise.
- **Simple exercise:** A planned rehearsal of a possible incident designed to evaluate an organization's capability to manage that incident and to provide an opportunity to improve the organization's future responses and enhance the relevant competences of those involved.
- **Drill:** Coordinated, supervised activities usually employed to exercise a single specific operation, procedure, or function in a single agency.
- **Simulation:** An exercise in which a group of players, usually representing a control center or management team, react to a simulated incident notionally happening elsewhere.
- **Live play:** An exercise activity that is as close as safely practicable to the expected response to a real incident. For the most comprehensive form of this exercise, referred to as full interruption, operations are shut down at the primary site and shifted to the recovery site in accordance with the disaster recovery plan.



Cybersecurity Book Resource Site https://app.box.com/v/ws-cybersecurity

Depending on the size and needs of an organization, management may choose to use one or more types of exercises. The responsible person or group, such as a business continuity manager, should determine one or more scenarios to guide exercise participants and encourage the usage of, review, and feedback on the business continuity plans. The following are examples of scenarios:

- **Loss of facility:** Continuing the delivery of critical products and services following the loss of a key facility (for example, due to fire)

https://t.me/learningnets

- **Loss of people:** Continuing the delivery of critical products and services with a reduced workforce (for example, due to pandemic)
- **Loss of technology:** Continuing the delivery of critical products and services without access to technology or systems (for example, due to data center failure)
- **Loss of equipment:** Continuing the delivery of critical products and services following the loss of key equipment (such as a metal press)
- **Loss of suppliers:** Continuing the delivery of critical products and services (such as payroll processing)

Tests

The objective of testing is to identify and address business continuity plan deficiencies by validating one or more of the system components and the operability of the plan. Testing takes several forms and accomplishes several objectives. Make sure it is conducted in an environment that is as similar to the operating environment as possible. FEMA's *Continuity Guidance for Non-Federal Entities* [FEMA09] lists the following as guidelines for testing:

- Annual testing (at a minimum) of alert, notification, and activation procedures for continuity personnel
- Annual testing of plans for recovering vital records, critical information systems, services, and data
- Annual testing of primary and backup infrastructure systems and services (for example, for power, water, and fuel) at continuity facilities
- Annual testing and exercising of required physical security capabilities
- Testing and validating of equipment to ensure the internal and external interoperability and viability of communications systems
- Annual testing of the capabilities required to perform an organization's essential functions
- A process for formally documenting and reporting tests and their results
- Annual testing of internal and external interdependencies identified in an organization's continuity plan, with respect to performance of the organization's and other organizations' essential functions

https://t.me/learningnets

Planning for an Exercise or a Test

Exercise and test planning is dictated by the objectives for testing defined in the BCP. Each individual exercise or test plan should identify quantifiable measurements of the exercise or test objective. Include the following items in your plan for an exercise or a test:

- **Goal:** Specifies the business continuity function or component of the BCP to be tested.
- **Objectives:** List the anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic, and timely.
- **Scope:** Identifies the departments or organizations involved, the critical business function, the geographic area, and the test conditions and presentation.
- **Artificial aspects and assumptions:** Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability.
- **Participant instructions:** Explains that the exercise provides an opportunity to test the BCP before an actual disaster.
- **Exercise or test narrative:** Gives participants the necessary background information, sets the environment, and prepares participants for action. It is important to include factors such as time, location, method of discovery, and sequence of events, whether events are finished or still in progress, initial damage reports, and any external conditions.
- **Evaluation:** Determines whether objectives were achieved, based on impartial monitoring. Participants' performance, including attitude, decisiveness, command, coordination, communication, and control are assessed. Debriefing is short yet comprehensive, explaining what did and did not work and emphasizing successes and opportunities for improvement. Be sure to include participant feedback in the exercise evaluation.

Performance Evaluation

Performance evaluation assesses the alignment of the BCMS (the operations of the BCMS as well as the planning process) to management requirements and the requirements in standards such as ISO 22301. ISO 22301 includes three key performance evaluation requirements:

- Establish, monitor, analyze, evaluate, and update metrics to assess performance of the BCMS at regular intervals

https://t.me/learningnets

- Establish and maintain an internal audit process to ensure that the BCMS aligns with management expectations and ISO 22301
- Communicate the performance of the BCMS and its solutions to program sponsors and other top management representatives through the management review process, with the objective of prioritizing continual improvement opportunities

Performance Metrics

Feedback derived from metrics guides management to prioritized ongoing improvement and adjustment to business continuity procedures. Good business continuity metrics have the following characteristics:

- Help senior managers (and/or their target audience) quickly see the performance of the response and recovery solutions based on risk to the organization's products and services
- Convey information that is important to senior managers
- Focus on performance rather than exclusively on activities
- Assist senior management in identifying problem areas to focus attention and remediation efforts

Table 17.2, based on FEMA's *Continuity Guidance for Non-Federal Entities* [FEMA09], provides a list of metrics that an organization can use to measure its ability to meet its continuity requirements. For each of the seven continuity considerations, management should use a simple grading system to show status, as defined in the table, using green for success, yellow for mixed results, and red for unsatisfactory.

TABLE 17.2 Continuity Considerations and Metrics

Continuity Requirements	Key Questions	Metrics
The continuation of the performance of essential functions during any emergency should be for a period up to 30 days or until normal operations are resumed and the capability to be fully operational at alternate sites as soon as possible after the occurrence of an emergency but not later than 12 hours after COOP activation.	■ Is your organization able to perform its current essential functions during any emergency and for up to 30 days or resumption of normal operations? ■ Is your organization able to be fully operational at an alternate site within 12 hours of COOP activation?	■ Measure ability to perform essential functions through test, training and exercise, identifying gaps and solutions. ■ Measure capability to be fully operational at a COOP site within 12 hours through testing, training, and exercises, identifying gaps and solutions.

https://t.me/learningnets

Continuity Requirements	Key Questions	Metrics
Plan and document succession orders and preplanned devolution of authorities that ensure the emergency delegation of authority in advance, in accordance with applicable law.	■ Does your organization have accessible and complete orders of succession that are familiar to successors? ■ Does your organization have accessible and complete devolution of authorities known by those to whom they devolve?	■ Document and train on succession orders. ■ Document and train on devolution of authorities.
Safeguard vital resources, facilities, and records.	■ Are your vital resources safeguarded? ■ Are your facilities safeguarded? ■ Are your records safeguarded? ■ Will your continuity staff have official access to your vital resources, facilities, and records in an emergency?	■ Document measures to safeguard vital resources, facilities, and records. ■ Document measures taken to ensure official access to vital resources, facilities, and records.
Make provisions for the acquisition of the resources necessary for continuity operations on an emergency basis.	■ Have you identified emergency continuity resources? ■ Do you have agreements/contracts to acquire emergency continuity resources?	■ Identify your emergency continuity resource requirements. ■ Identify what agreements/contracts you have made to meet these requirements. ■ Identify what additional agreements/contracts are needed.
Make provisions for the availability and redundancy of critical communications capabilities at alternate sites in order to support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public.	■ Do you have critical communications capability at your alternate site(s)? ■ Do you have redundant communications capability at your alternate site(s)?	■ Identify your current communications capability at your alternate site. ■ Identify what communications capability is necessary. ■ Identify the plan to improve communications at your alternate site in six months, one year, and two years.

https://t.me/learningnets

Continuity Requirements	Key Questions	Metrics
Make provisions for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations.	■ What is your plan for ensuring your reconstitution capability?	■ Identify your reconstitution capability plan.
Make provisions for the identification, training, and preparedness of personnel capable of relocating to continuity facilities to support the continuation of the performance of essential functions.	■ Have you identified, trained, and prepared personnel to relocate to alternate sites to continue essential functions?	■ Verify that staff are identified, trained, and prepared to relocate to alternate sites.

ISO 22313 lists the following requirements for monitoring performance:

- Setting of performance metrics, including qualitative and quantitative measurements that are appropriate to the needs of the organization
- Monitoring the extent to which the organization's business continuity policy and objectives are met
- Identifying when monitoring and measuring should take place
- Assessing the performance of the processes, procedures, and functions that protect prioritized activities
- Putting in place proactive measures of performance that monitor compliance of the BCMS with applicable legislation, statutory, and regulatory requirements
- Putting in place reactive measures of performance to monitor failures, incidents, nonconformances (including near misses and false alarms), and other historical evidence of deficient BCMS performance
- Recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective action analysis

Internal Audit

An organization should implement an internal audit process for business continuity, whose purpose is to evaluate the performance of the BCMS. This does not necessarily mean that an internal audit department is needed or has this task. An audit needs to be performed by some knowledgeable person or group independent of the BCMS. An organization should scale the depth and frequency of audit activities and reporting to the assessed importance of business continuity. While the scope of audit activities and

https://t.me/learningnets

deliverables may vary, in all cases they must encompass an independent and objective evaluation of the effectiveness of the BCMS.

Key tasks for internal auditing are as follows:

- Ensure that the audit program is capable of determining whether the BCMS conforms to requirements
- Ensure that the audit program is capable of determining whether the BCMS conforms to the BC plan
- Establish and implement the audit program
- Ensure that top management reviews the effectiveness of the audit program

Management Review

Management review is an essential aspects of business continuity management. Such a review needs to evaluate readiness and conformance to requirements and standards. The management review needs to address the following points:

- Results of BCM audits; post-emergency, crisis, or disaster reviews; and exercise results
- BCM status of key suppliers and outsource partners, as available
- Level of remaining and acceptable risks
- Inadequately managed risks, including those identified in the entity's previous risk assessment
- Internal or external changes likely to affect the entity's BCM capability
- Results of exercises, tests, and self-assessments
- Accomplishments of training and awareness programs
- Follow-up procedures based on previous management reviews
- Proposed recommendations for development of the entity's BCM capability

An organization should include the following in the review document:

- Scope of the review
- Reasons for the review
- People involved in the review
- Areas where issues exist, especially any raised risks
- Recommendations for corrective and preventive actions
- Brief review of tests and exercises

https://t.me/learningnets

17.4 Business Continuity Operations

As depicted in Figure 17.1, business continuity operations constitutes the foundation layer for business continuity management. In response to a disruptive event, the business continuity process proceeds in three overlapping phases (see Figure 17.6):

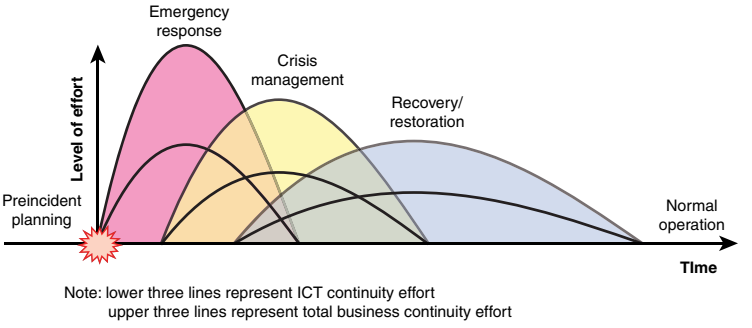


FIGURE 17.6 Business Continuity Process

1. **Emergency response:** Focused on arresting or stabilizing an event
2. **Crisis management:** Focused on safeguarding the organization
3. **Business recovery/restoration:** Focused on fast restoration and recovery of critical business processes

Figure 17.6 provides a rough indication of the typical level of effort and time scale for each phase. The relative values depend on the nature and severity of the incident, the complexity of the organization, and the organization's state of readiness.

Emergency Response

An emergency response is an urgent response to a fire, flood, civil commotion, natural disaster, bomb threat, or other serious situation, with the intent of protecting lives, limiting damage to property, and minimizing disruption of system operations.

Generally, an emergency response is of limited duration—usually minutes to hours. Key tasks performed by designated emergency response personnel include:

- Account for staff and visitors
- Deal with casualties
- Contain/limit damage

https://t.me/learningnets

- Assess damage
- Invoke the business continuity plan by contacting the crisis management team point of contact

The nature of a security incident dictates which personnel are involved in the emergency response. For example, in the case of a fire alarm, generally all staff have been instructed on the evacuation procedure to a gathering point safe area. One person or one staff position per building or floor can be assigned the job takeoff taking a roll call at the gathering point. This should be a person designated to confirm that the fire department has received the alarm and is responding. From that point, a crisis manager team leader may take over the task of coordinating the business continuity response.

As another example, to deal with a power outage, an emergency response team can be designated for the data center. One member of the team should verify that the backup generator is operating properly and check with the service provider for a status report. If power is restored before any further action is needed, then the incident is closed. If the power outage is prolonged, the emergency response team may inform the crisis management team so that the crisis management team coordinates an offsite location with a current mirror image of the data center and takes any other business continuity tasks required as the incident unfolds.

Crisis Management

Crisis management involves ensuring that processes, controls, and resources are available immediately following a disruption to ensure that the enterprise continues to deliver its critical business services.

Typically, crisis management occurs over a time frame of hours to days. Key tasks performed by the crisis management team include the following:

- Contacting staff, customers, and suppliers, as needed
- Performing the initial recovery of critical business processes to the extent possible
- Rebuilding lost work in progress

A crisis management team needs to react quickly. This should be a small group of a dozen or fewer individuals who can easily coordinate among themselves. This team must include individuals who have the authority to provide corporate leadership and direct business continuity activities during times of crisis or in emergencies. Table 17.3, from *Business Continuity Management Guidelines* [WAG15], shows the makeup of a typical crisis management team.

https://t.me/learningnets

TABLE 17.3 Crisis Management Team

Role	Responsibilities
Crisis manager/team leader	■ Provides overall leadership ■ Liaises with board and CEO ■ Allocates resources, sets priorities, and resolves conflicts ■ Briefs the company spokesperson
Command center coordinator	■ Keeps the command center functioning, including supporting technologies and resources ■ Maintains the status board for the crisis and call register
Corporate communications staff	■ Act as a single source of information to internal and external stakeholders and media ■ Provide media management
Human resources staff	■ Provide employee assistance, such as medical assistance, counseling, insurance claims, payroll duties, and so on. ■ Handle emergency evacuation/repatriation ■ Liaise with victims' families ■ Provide recruitment support
Corporate security staff	■ Ensure staff safety ■ Liaise with emergency services ■ Monitor emergency response ■ Provide for security of assets and staff ■ Communicate with external parties on security intelligence
Administration and logistics support staff	■ Facilitate and supports recovery efforts, possibly consisting of food services, transport arrangements, mail duties, insurance, legal, finance requirements, and so on
Premises and facilities staff	■ Coordinate damage assessment, salvage and repair operations, and reconstruction ■ Support the insurance claim process ■ Plan for relocation to the primary site
Business recovery coordinator	■ Coordinates execution of business recovery plans ■ Provides status updates to the crisis management team
IT recovery coordinator	■ Coordinates execution of IT recovery plans ■ Resolves system, network, and application issues ■ Provides status updates to the crisis management team

Business Recovery/Restoration

Business recovery/restoration is aimed at getting the enterprise back to normal operation as soon as practical. Typically, business recovery/restoration occurs over a time

https://t.me/learningnets

frame of days to weeks or possibly even months. Key tasks performed by the crisis management team include the following:

- Damage repair/replacement
- Relocation to a permanent place of work
- Restoration of normal IT operations
- Recovery of costs from insurers

Business recovery/restoration may involve a number of teams, depending on the size and complexity of the organization, and the teams may be organized on functional or departmental lines. Table 17.4, from *Business Continuity Management Guidelines* [WAG15], shows the makeup of a typical business recovery/restoration team.

TABLE 17.4 Response/Recovery Team

Role	Responsibilities
Team leader	■ Provides overall leadership to the team ■ Ensures that critical activities are restored within the required time frames ■ Keeps the crisis management team appraised of business continuity progress
Alternate team leader	■ Acts as a backup to the team leader
BCM coordinator	■ Assists the team leader, as required ■ Coordinates communications within the team and liaises with other areas of the agency ■ Maintains a status board on the team's business continuity progress
Team members	■ Carry out business continuity tasks in accordance with the team's business continuity and recovery plan
Standby team members	■ Are on standby at home ■ Provide assistance with business continuity tasks when called upon ■ Support long-term recovery task when required

In addition to the activities that are specific to the various recovery/restoration teams and the crisis management team, all team leaders need to address the following common concerns:

- Ensure that all local activities and dependencies are addressed by the plans.
- Have administrative responsibility for the plans.
- Coordinate routine updates to the detailed information supporting the crisis management and recovery response procedures (for example, risk assessments, contact lists, personnel assignments, hardware and software specifications, network diagrams, vital records, inventory lists, offsite backup schedules).

https://t.me/learningnets

- Coordinate electronic access to, and hard copy distribution of, the relevant plans and procedures to personnel who need them.
- Ensure that relevant persons are aware of the plans and their role in any post-disruption activities identified by the plans.
- Protect the confidentiality, integrity, and availability of the emergency response and business continuity plans and associated procedures.
- Ensure that service agreements with other stakeholders, emergency services, and business continuity service providers are agreed and in place.
- Ensure that out-of-hours emergency responsibilities are addressed and understood.

The flowchart in Figure 17.7 provides a general picture of the relationship between security incident management, emergency response, crisis management, and recovery/restoration.

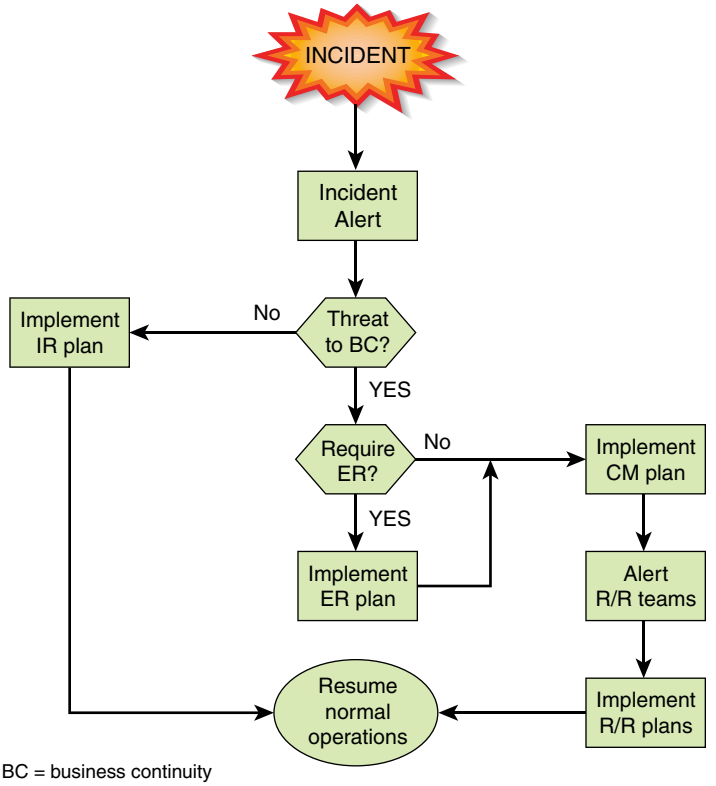


FIGURE 17.7 Incident Response and Business Continuity

https://t.me/learningnets

17.5 Business Continuity Best Practices

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) breaks down the best practices in the business continuity category into two areas and seven topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Business continuity framework:** The objective of this area is to develop an organizationwide business continuity strategy and program that is supported by a resilient technical infrastructure and an effective crisis management capability.
  - **Business continuity strategy:** Provides a checklist of actions for developing a business continuity strategy similar in nature to the actions for developing an information security strategy.
  - **Business continuity program:** Provides guidance on defining the business continuity requirements for each business environment.
  - **Resilient technical environments:** Describes techniques for ensuring resilience, including resilient hardware/software, redundancy, isolation, and backups.
  - **Crisis management:** Provides a checklist of elements that should be part of a crisis management plan.
- **Business continuity process:** The objective of this area is to develop, maintain, and regularly test business continuity plans and arrangements (sometimes referred to as *disaster recovery plans*) for critical business processes and applications throughout the organization.
  - **Business continuity planning:** Describes all the elements that should be included in a business continuity plan, including risk assessment, assignment of roles, metrics to be met, and the process of responding to an incident that threatens business continuity.
  - **Business continuity arrangements:** Lists the elements that should be included in a disaster recovery plan.
  - **Business continuity testing:** Describes an approach to testing business continuity plans.

https://t.me/learningnets

17.6 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

accessibility
autonomic computing
awareness
business continuity
business continuity management (BCM)
business continuity management system (BCMS)
business continuity manager
business continuity plan
business continuity program
business continuity readiness
business continuity strategy
business impact analysis
business recovery/restoration
business resilience
continuity of operations (COOP)
crisis management
drill
diversification
emergency response
exercise
hardening
information system resilience
internal audit
live play
management review
maximum tolerable downtime (MTD) performance evaluation
performance metrics recovery
recovery point objective (RPO)
recovery time objective (RTO)
redundancy
resilience
risk assessment
simple exercise
simulation
tabletop exercise
training

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Describe the three key elements of business continuity.
2. What natural disaster threats can disrupt business continuity?
3. What human-caused disasters can disrupt business continuity?
4. What are the four key business components that are critical for maintaining business continuity?
5. What are the key steps of business impact analysis?
6. According to ISO 22301, what are three key areas to consider while developing a business continuity strategy?

https://t.me/learningnets

7. What are the key objectives of a business continuity awareness program?
8. Briefly define the term *business resilience*.
9. Define five sets of organizational continuity controls.
10. List some improvement exercises for participants in an ideal BCP.
11. What are the characteristics of good business continuity metrics?
12. What are the three phases of the business continuity process in response to a disruptive event?

17.7 References

ENIS10: European Union Agency for Network and Information Security, *ENISA IT Business Continuity Management: An Approach for Small and Medium Sized Organizations.* January 2010. https://www.enisa.europa.eu/publications/business-continuity-for-smes/at_download/fullReport

FEMA09: Federal Emergency Management Agency, *Continuity Guidance for Non-Federal Entities (States, Territories, Tribal and Local Government Jurisdictions, and Private Sector Organizations)*. Continuity Guidance Circular 1 (CGC 1), January 21, 2009.

FFIE15: Federal Financial Institutions Examination Council, *Business Continuity Planning*. February 2015.

GOBL02: Goble, G., Fields, H., & Cocchiara, R., *Resilient Infrastructure: Improving Your Business Resilience.* IBM Global Service White Paper. September 2002.

NCEM12: National Emergency Crisis and Disasters Management Authority, *Business Continuity Management Standard and Guide.* United Arab Emirates Supreme Council for National Security Standard AE/HSC/NCEMA 7000, 2012. https://www.ncema.gov.ae/content/documents/BCM%20English%20NCEMA_29_8_2013.pdf

WAG15: Western Australian Government, *Business Continuity Management Guidelines*. June 2015. https://www.icwa.wa.gov.au/__data/assets/pdf_file/0010/6112/Business-Continuity-Management-Guidelines.pdf

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

https://t.me/learningnets

PART III

Security Assessment

In return for all this we asked but one condition: that was, that you should embrace the true faith, and conform in every way to its usages. This you promised to do, and this, if common report says truly, you have neglected.

—A Study in Scarlet, Sir Arthur Conan Doyle

CHAPTER 18: Security Monitoring and Reporting

Part III discusses techniques for auditing and monitoring the performance of cybersecurity controls, with a view to spotting gaps in the system and devising improvements. The only chapter, Chapter 18, covers security auditing as well as evaluating security performance.

https://t.me/learningnets

Chapter 18

Security Monitoring and Improvement

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

—*The Art of War*, Sun Tzu

Learning Objectives

After studying this chapter, you should be able to:

- Present the X.816 model of security audit and alarms.
- List useful information to collect in security audit trails.
- Discuss security audit controls.
- Understand the use of metrics in security performance monitoring.
- Describe the essential elements of information risk reporting.
- Discuss what is involved in information security compliance monitoring.
- Present an overview of security monitoring and improvement best practices.

This chapter looks at two aspects of security monitoring that lead to improvement in organizational security: the security audit and security performance.

18.1 Security Audit

In general terms, an audit in an enterprise is an independent inspection of enterprise records to determine compliance with a standard or policy. More specifically, a **security audit** relates to security policies and the mechanisms and procedures used to enforce that policy. A **security audit trail** is an important component of a security audit.

https://t.me/learningnets

X.816, *Security Audit and Alarms Framework*, lists the following objectives for a security audit:

- Allows the adequacy of the security policy to be evaluated
- Aids in the detection of security violations
- Facilitates making individuals accountable for their actions (or for actions by entities acting on their behalf)
- Assists in the detection of misuse of resources
- Acts as a deterrent to individuals who might attempt to damage the system

security audit
An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

security audit trail
A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Security audit mechanisms are not involved directly in the prevention of security violations. Rather, they are concerned with the detection, recording, and analysis of events. The basic objective of a security audit is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate security violations.

Security Audit and Alarms Model

X.816 has developed a model that shows the elements of the security auditing function and their relationships to security alarms (see Figure 18.1).

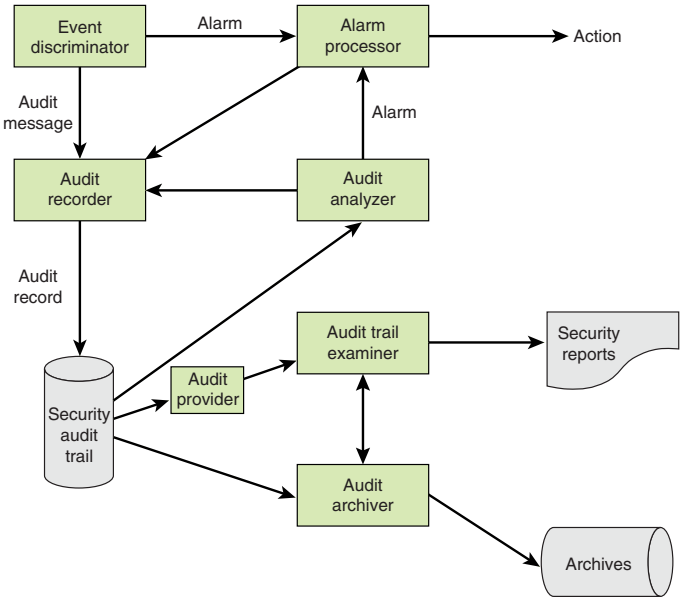


FIGURE 18.1 Security Audit and Alarms Model

https://t.me/learningnets

The key elements of this model are as follows:

- **Event discriminator:** This logic embedded in the software of the system monitors system activity and detects security-related events that it was configured to detect.
- **Audit recorder:** For each detected event, the event discriminator transmits the information to an audit recorder. The model depicts this transmission in the form of a message. The audit could also be done by recording the event in a shared memory area.
- **Alarm processor:** Some of the events detected by the event discriminator are defined to be alarm events. For such events, an alarm is issued to an alarm processor. The alarm processor takes some action based on the alarm. This action is itself an auditable event and so is transmitted to the audit recorder.
- **Security audit trail:** The audit recorder creates a formatted record of each event and stores it in the security audit trail.
- **Audit analyzer:** The security audit trail is available to the audit analyzer, which, based on a pattern of activity, may define a new auditable event that is sent to the audit recorder and may generate an alarm.
- **Audit archiver:** This software module periodically extracts records from the audit trail to create a permanent archive of auditable events.
- **Archives:** The audit archives are a permanent store of security-related events on this system.
- **Audit provider:** The audit provider is an application and/or user interface to the audit trail.
- **Audit trail examiner:** The audit trail examiner is an application or a user who examines the audit trail and the audit archives for historical trends, for computer forensic purposes, and for other analyses.
- **Security reports:** The audit trail examiner prepares human-readable security reports.

As shown, the auditing process begins with the detection of security-related events, which may in turn be determined to be security incidents that produce alarms. Refer to Figure 15.3 in Chapter 15, "Threat and Incident Management," for details of this process.

Data to Collect for Auditing

The choice of what data to collect should be based on a number of requirements. One issue is the amount of data to collect, which is determined by the range of areas of

https://t.me/learningnets

interest and by the granularity of data collection. There is a trade-off here between quantity and efficiency. The more data collected, the greater the performance penalty on the system. Larger amounts of data may also unnecessarily burden the various algorithms used to examine and analyze the data. Further, the presence of large amounts of data creates a temptation to generate security reports excessive in number or length.

With these cautions in mind, the first order of business in security audit trail design is the selection of data items to capture, including the following:

- Events related to the use of the auditing software (that is, all the components in Figure 18.1)
- Events related to the security mechanisms on the system
- Any events that are collected for use by the various security detection and prevention mechanisms, including items related to intrusion detection and items related to firewall operation
- Events related to system management and operation
- Events related to operating system access (for example, via system calls)
- Events related to application access for selected applications
- Events related to remote access

X.816 suggests the auditing the following:

- Security events related to a specific connection:
  - Connection requests
  - Connection confirmed
  - Disconnection requests
  - Disconnection confirmed
  - Statistics appertaining to the connection
- Security events related to the use of security services:
  - Security service requests
  - Security mechanisms usage
  - Security alarms
- Security events related to management:
  - Management operations
  - Management notifications

https://t.me/learningnets

The list of auditable events should include at least the following:

- Deny access
- Authenticate
- Change attribute
- Create object
- Delete object
- Modify object
- Use privilege

In terms of the individual security services, the following security-related events are important:

- **Authentication:** Verify success and verify fail
- **Access control:** Decide access success and decide access fail
- **Non-repudiation:** Non-repudiable origination of message, non-repudiable receipt of message, unsuccessful repudiation of event, and successful repudiation of event
- **Integrity:** Use of shield, use of unshield, validate success, and validate fail
- **Confidentiality:** Use of hide and use of reveal
- **Audit:** Select event for auditing, deselect event for auditing, and change audit event selection criteria

The standard points out that both normal and abnormal conditions may need to be audited; for instance, each connection request, such as a Transmission Control Protocol (TCP) connection request, may be a subject for a security audit trail record, whether or not the request was abnormal and regardless of whether the request was accepted. This is an important point. Data collection for auditing goes beyond the need to generate security alarms or to provide input to a firewall module. Data representing behavior that does not trigger an alarm are used to identify normal versus abnormal usage patterns and thus serve as input to intrusion detection analysis. Also, in the event of an attack, an analysis of all the activity on a system may be needed to diagnose the attack and arrive at suitable countermeasures for the future.

As a security administrator designs an audit data collection policy, it is useful to organize the audit trail into categories for purposes of choosing data items to collect. The following sections look at categories for audit trail design.

https://t.me/learningnets

System-Level Audit Trails

System-level audit trails are generally used to monitor and optimize system performance but serve a security audit function as well. The system enforces certain aspects of security policy, such as access to the system itself. A system-level audit trail captures data such as login attempts (both successful and unsuccessful), devices used, and operating system functions performed. Other system-level functions may be of interest for auditing, such as system operation and network performance indicators.

Application-Level Audit Trails

Application-level audit trails are used to detect security violations in an application or to detect flaws in the application's interaction with the system. For critical applications, or those that deal with sensitive data, an application-level audit trail provides the desired level of detail to assess security threats and impacts. For example, for an e-mail application, an audit trail records sender and receiver, message size, and types of attachments. An audit trail for a database interaction using Structured Query Language (SQL) queries records the user, type of transaction, and even individual tables, rows, columns, or data items accessed.

User-Level Audit Trails

A user-level audit trail traces the activity of an individual user over time. It is used to hold a user accountable for his or her actions. Such audit trails are also useful as input to an analysis program that attempts to define normal versus anomalous behavior.

A user-level audit trail records user interactions with the system, such as commands issued, identification and authentication attempts, and files and resources accessed. The audit trail also captures the user's use of applications.

Network-Level Audit Trails

Network-level audit trails encompass a wide variety of network activity. Enterprises use such audit trails to evaluate system performance and perform load balancing. These audit trails can also include security-related data, such as that generated by firewalls, virtual private network managers, and IPsec traffic.

Physical Access Audit Trails

Physical access audit trails are generated by equipment that controls physical access and are then transmitted to a central host for subsequent storage and analysis.

https://t.me/learningnets

Examples are card-key systems and alarm systems. The following are examples of the types of data of interest:

- Log the date and time the access was attempted or made as well as the gate or door through which the access was attempted or made, as well as the individual (or user ID) making the attempt to access the gate or door.
- Monitor and log invalid attempts by non-computer audit trails just as you would for computer system audit trails. Make sure management is aware that someone is attempting to gain access during unauthorized hours.
- Log information that also includes attempts to add, modify, or delete physical access privileges (for example, granting a new employee access to the building or granting transferred employees access to their new office—and, of course, deleting their old access, as applicable).
- As with system and application audit trails, implement auditing of non-computer functions to send messages to security personnel indicating valid or invalid attempts to gain access to controlled spaces. A guard or monitor may be desensitized if all access results in messages being sent to a screen. Therefore, it is best to highlight only exceptions, such as failed access attempts, to those monitoring access.

Where appropriate, the log data can include digital archives of video surveillance contemporaneous with a logged event.

Internal and External Audit

internal security audit
An audit conducted by personnel responsible to the management of the organization being audited.

external security audit
An audit conducted by an organization independent of the one being audited.

A sound auditing policy includes both **internal security audits** and **external security audits**. Internal audits are carried out by the organization itself, typically on a quarterly basis or after a significant security event. External audits are carried out by someone from outside, typically on annual basis.

The objectives of an internal security audit include the following:

- Identify security weaknesses
- Provide an opportunity to improve the information security management system
- Provide management with information about the status of security
- Deliver information about the status of security to management
- Review compliance of security systems with the information security policy of the organization
- Find and resolve noncompliance

https://t.me/learningnets

The objectives of the external security include the following:

- Assess the process of the internal audit
- Determine the commonality and frequency of recurrence of various types of security violations
- Identify the common causes of various types of security violations
- Provide advisory and training inputs to tackle the neglect of procedures
- Review and update the policy

Security Audit Controls

A useful guide to developing a security audit program is the family of audit controls defined in SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. The controls are designed to be flexible and customizable and implemented as part of an organizationwide process to manage risk.

The audit and accountability family consists of 16 base controls. Some of the base controls include one or more control enhancements, which add functionality or specificity to a base control or increase the strength of a base control. The control enhancements are labeled with numbers in parentheses in the following list and table. In the following list some numbers associated with control enhancements are missing; these are withdrawn enhancements. The 16 base controls are:

- **Audit and accountability policy and procedures:** Defines the governance strategy for a security audit policy.
- **Audit events:** This control includes specifying the type of events to be audited. Additional guidance for this control includes the following: Specify the event types to be audited; Verify that the system can audit the selected event types; provide a rationale for why the auditable event types are deemed to be adequate to support after-the-fact investigations of security and privacy incidents; and coordinate the security audit function with other organizational entities requiring audit-related information.
  - (3) Periodically review and update the set of events to be audited.
- **Content of audit records:** Deals with the content of audit records, including the following issues:
  - (1) Specify the content of an audit record, such as what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

https://t.me/learningnets

- (2) Provide centralized management and configuration of the content to be captured.
- (3) Limit the personally identifiable information contained in audit records.

- **Audit storage capacity:** Deals with allocating sufficient storage capacity to accommodate record retention requirements.
  - (1) Periodically offload audit records onto a different system or media.
- **Response to audit processing failures:** Provides guidance on alerting specific personnel about an audit processing failure and what additional actions to take. The following control enhancements are covered:
  - (1) Provide warning when allocated storage is exhausted.
  - (2) Provide an alert to designated personnel or locations when specified audit failure events occur.
  - (3) Enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity.
  - (4) Invoke a specified full system shutdown, partial system shutdown, or degraded operational mode with limited mission/business functionality available in the event of specified audit processing failures.
- **Audit review, analysis, and reporting:** Deals with reviewing and analyzing security audit records at a specified frequency, with reports to specified individuals. Enhancement include:
  - (1) Employ automated mechanisms to integrate audit review, analysis, and reporting.
  - (3) Analyze and correlate audit records across different repositories to gain organizationwide situational awareness.
  - (4) Provide and implement the capability to centrally review and analyze audit records from multiple components in the system.
  - (5) Integrate analysis of audit records with other security analysis and monitoring efforts.
  - (6) Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.
  - (7) Specify permitted actions for system processes, roles, and/or users associated with the review, analysis, and reporting of audit records.
  - (8) Require a distinct environment for the dedicated analysis of audit information related to privileged users.
  - (9) Correlate information from nontechnical sources with audit information to enhance organizationwide situational awareness.

https://t.me/learningnets

- **Audit reduction and report generation:** Deals with providing summary information from audit records that is meaningful to analysts. May also include:
  - (1) Provide and implement the capability to process audit records for events of interest based on specified criteria.
  - (2) Provide and implement the capability to sort and search audit records for events of interest based on selected audit fields.
- **Time stamps:** Deals with recording time stamps from internal system clocks. Enhancements include:
  - (1) Synchronize with an authoritative time source.
  - (2) Identify a secondary authoritative time source to be used if the primary source is not available.
- **Protection of audit information:** Deals with providing technical or automated protection of audit information. Enhancements include:
  - (1) For initial generation and backup of audit trails, use hardware-enforced, write-once media.
  - (2) Store audit information in a repository separate from the audited system or system component.
  - (3) Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
  - (4) Authorize access to management of audit functionality to only selected privileged users.
  - (5) For executing selected actions, require the approval of two authorized individuals.
  - (6) Authorize read-only access to audit information to a selected subset of privileged users.
  - (7) Store audit information on a component running a different operating system than the system or component being audited.
- **Non-repudiation:** Deals with protecting against an individual falsely denying having performed selected audit-related activities. Enhancements include:
  - (1) Provide organizational personnel with the means to identify who produced specific information in the event of an information transfer.
  - (2) Prevent the modification of information between production and review.
  - (3) Maintain reviewer or releaser identity and credentials within the established chain of custody for all information reviewed or released.
  - (4) Prevent the modification of information between review and transfer/release.

https://t.me/learningnets

- **Audit record retention:** Provides guidance for developing a record retention policy.
  - (1) Employ organization-defined measures to ensure that long-term audit records generated by the system can be retrieved.
- **Audit generation:** Provides guidance for defining an audit record generation capability for the auditable event types. Enhancements include:
  - (1) Compile audit records from organization-defined system components into a systemwide audit trail that is time-correlated to within the organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.
  - (2) Produce a systemwide (logical or physical) audit trail composed of audit records in a standardized format.
  - (3) Extend or limit auditing, as necessary, to meet organizational requirements. Auditing that is limited to conserve system resources may be extended to address certain threat situations.
  - (4) Audit query parameters within systems for data sets that contain personally identifiable information; this augments an organization's ability to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.
- **Monitoring for information disclosure:** Discusses monitoring open source information (for example, from social networking sites) for evidence of unauthorized disclosure of organizational information. Enhancements include:
  - (1) Employ automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.
  - (2) Review the open source information sites being monitored.
- **Session audit:** Deals with providing and implementing the capability for authorized users to select a user session to capture/record or view/hear. Enhancements include:
  - (1) Initiate session audits automatically at system startup.
  - (2) Provide and implement the capability for authorized users to capture, record, and log content related to a user session.
  - (3) Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.
- **Alternate audit capability:** Deals with providing an alternate audit capability in the event of a failure in primary audit capability that implements organization-defined alternate audit functionality.

https://t.me/learningnets

- **Cross-organizational audit:** When organizations use systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. This control provides for such a capability. Enhancements include:
  - (1) Require that the identity of individuals be preserved in cross-organizational audit trails.
  - (2) Provide cross-organizational audit information to organization-defined organizations based on organization-defined cross-organizational sharing agreements.

This set of controls provides comprehensive guidance for planning and implementing an effective security auditing function.

Table 18.1 lists the recommended set of minimum security controls, called a *control baseline*. Section 16.2 in Chapter 16, "Local Environment Management," describes the concept of control baselines. Table 18.1 provides additional guidance for an organization in selecting controls based on risk assessment.

TABLE 18.1 Audit and Accountability Control Baseline

Control		Control Baselines		
		Low	Moderate	High
AU-1	Audit and accountability policy and procedures	AU-1	AU-1	AU-1
AU-2	Audit events	AU-2	AU-2(3)	AU-2(3)
AU-3	Content of audit records	AU-3	AU-3(1)	AU-3(1)(2)
AU-4	Audit storage capacity	AU-4	AU-4	AU-4
AU-5	Response to audit processing failures	AU-5	AU-5	AU-5(1)(2)
AU-6	Audit review, analysis, and reporting	AU-6	AU-6(1)(3)	AU-6 (1)(3)(5)(6)
AU-7	Audit reduction and report generation	—	AU-7(1)	AU-7(1)
AU-8	Time stamps	AU-8	AU-8(1)	AU-8(1)
AU-9	Protection of audit information	AU-9	AU-9(4)	AU-9 (2)(3)(4)
AU-10	Non-repudiation	—	—	AU-10
AU-11	Audit record retention	AU-11	AU-11	AU-11
AU-12	Audit generation	AU-12	AU-12	AU-12(1)(3)
AU-13	Monitoring for information disclosure	—	—	—
AU-14	Session audit	—	—	—
AU-15	Alternate audit capability	—	—	—
AU-16	Cross-organizational audit	—	—	—

https://t.me/learningnets

18.2 Security Performance

Security performance is the measurable result of security controls applied to information systems and supporting information security programs. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) defines the security performance function as comprising three areas:

- **Security monitoring and reporting:** Consists of monitoring security performance regularly and reporting to specific audiences, such as executive management
- **Information risk reporting:** Consists of producing reports relating to information risk and presenting reporting to executive management on a regular basis
- **Information security compliance monitoring:** Consists of information security controls derived from regulatory and legal drivers and contracts, used to monitor security compliance

An essential element of security performance assessment is the selection of security performance metrics. This section looks first at the topic of security performance metrics and then treats the three areas previously listed.

Security Performance Measurement

Two terms are relevant to this discussion:

- **Security performance:** The measurable result of security controls applied to information systems and supporting information security programs.
- **Security performance metric:** A variable related to security performance to which a value is assigned as the result of measurement. Also called a **security performance measure**.

National Institute of Standards and Technology (NIST) IR 7564, *Directions in Security Metrics Research*, lists the following as the main broad uses of security metrics:

- **Strategic support:** Assessments of security properties can be used to aid in different kinds of decision making, such as program planning, resource allocation, and product and service selection.
- **Quality assurance:** Security metrics can be used during the software development life cycle to eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying vulnerabilities that are likely to exist, and tracking and analyzing security flaws that are eventually discovered.

https://t.me/learningnets

- **Tactical oversight:** Monitoring and reporting of the security status or posture of an IT system can be carried out to determine compliance with security requirements (for example, policies, procedures, regulations), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement.

Yee's article "Security Metrics: An Introduction and Literature Review" [YEE17] states that a security metrics should do the following:

- Measure quantities that are meaningful for establishing the security posture of a computer system or of an organization
- Be reproducible
- Be objective and unbiased
- Be able to measure a progression toward a goal over time

Sources of Security Metrics

A security officer or a group responsible for developing a set of metrics for security performance assessment draws on several authoritative sets, some of which are described here.

Chapter 1, "Best Practices, Standards, and a Plan of Action," discusses the organization of COBIT 5 into 5 domains and 37 processes. Relevant for the discussion of this chapter is the Monitor, Evaluate, and Assess (MEA) domain, which deals with a company's strategy in assessing the needs of the company and whether the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. Three processes comprise this domain:

- **Performance and conformance:** Collect, validate, and evaluate business, IT, and process goals and metrics. Monitor to ensure that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.
- **System of internal control:** Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize, and maintain standards for internal control assessment and assurance activities.

https://t.me/learningnets

- **Compliance with external requirements:** Evaluate whether IT processes and IT-supported business processes are compliant with laws, regulations, and contractual requirements. Obtain assurance that the requirements were identified and complied with and integrate IT compliance with overall enterprise compliance.

Table 18.2 lists the metrics defined for these three processes.

TABLE 18.2 Suggested Security Performance Metrics (COBIT 5 for Information Security)

Goal	Metrics
Performance and Conformance	
Information security performance is monitored on an ongoing basis	■ Percentage of business processes that meet defined information security requirements
Information security and information risk practices conform to internal compliance requirements.	■ Percentage of information security practices that satisfy internal compliance requirements
System of Internal Control	
Information security controls are deployed and operating effectively	■ Percentage of processes that satisfy information security control requirements ■ Percentage of controls in which information security control requirements are met
Monitoring processes for information security controls are in place and results are reported	■ Percentage of information security controls appropriately monitored and results reported and reviewed
Compliance with External Requirements	
Information security and information risk practices conform to external compliance requirements	■ Percentage of information security practices that satisfy external compliance requirements
Monitoring is conducted for new or revised external requirements with an impact on information security	■ Number or percentage of projects initiated by information security to implement new external requirements

SP 800-55, *Performance Measurement Guide for Information Security*, lists a number of candidate metrics that organizations can tailor, expand, or use as models for developing other metrics (see Table 18.3). The recommended metrics focus on the SP 800-53 security controls. In essence, the metrics measure the effectiveness of the implementation of the security controls.

https://t.me/learningnets

TABLE 18.3 Examples of Security Performance Metrics (NIST 800-55)

Area	Metric
Security budget	Percentage of the agency's information system budget devoted to information security
Vulnerability management	Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
Access control	Percentage of remote access points used to gain unauthorized access
Awareness and training	Percentage of information system security personnel that have received security training
Audit and accountability	Average frequency of audit records review and analysis for inappropriate activity
Certification, accreditation, and security assessments	Percentage of new systems that have completed certification and accreditation (C&A) prior to their implementation
Configuration management	Percentage approved and implemented configuration changes identified in the latest automated baseline configuration
Contingency planning	Percentage of information systems that have conducted annual contingency plan testing
Identification and authentication	Percentage of users with access to shared accounts
Incident response	Percentage of incidents reported within the required time frame, per applicable incident category
Maintenance	Percentage of system components that undergo maintenance in accordance with formal maintenance schedules
Media protection	Percentage of media that passes sanitization procedures testing for FIPS 199 high-impact systems
Physical and environmental	Percentage of physical security incidents allowing unauthorized entry into facilities containing information systems
Planning	Percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior
Personnel security	Percentage of individuals screened before being granted access to organizational information and information systems
Risk assessment	Percentage of vulnerabilities remediated within organization-specified time frames
System and services acquisition	Percentage of system and service acquisition contracts that include security requirements and/or specifications
System and communication protection	Percentage of mobile computers and devices that perform all cryptographic operations using FIPS 140-2–validated cryptographic modules operating in approved modes of operation
System and information integrity	Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated

https://t.me/learningnets

There is one metric for each system control. For each metric, SP 800-55 provides detailed guidance in a number of categories. For example, for the maintenance metric, these are the category values:

- **Goal:** *Strategic Goal:* Accelerate the development and use of an electronic information infrastructure. *Information Security Goal:* Perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- **Measure:** Percentage (%) of system components that undergo maintenance in accordance with formal maintenance schedules.
- **Measure Type:** Effectiveness/Efficiency
- **Formula:** (Number of system components that undergo maintenance according to formal maintenance schedules/total number of system components) × 100.
- **Target:** This should be a high percentage defined by the organization.
- **Implementation Evidence:** (1) Does the system have a formal maintenance schedule? (2) How many components are contained within the system? (3) How many components underwent maintenance in accordance with the formal maintenance schedule?
- **Frequency:** *Collection Frequency:* Organization-defined (example: quarterly); *Reporting Frequency:* Organization-defined (example: annually)
- **Responsible Parties:** *Information Owner:* Organization-defined (example: System Owner); *Information Collector:* Organization-defined (for example, system administrator); *Information Customer:* Chief information officer (CIO), information system security officer (ISSO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO])
- **Data Source:** Maintenance schedule, maintenance logs
- **Reporting Format:** Pie chart comparing the percentage of system components receiving maintenance in accordance with the formal maintenance schedule versus the percentage of system components not receiving maintenance in accordance with the formal maintenance schedule over the specified period

Chapter 1 discusses the critical security controls defined by the Center for Internet Security (CIS) (refer to Table 1.10). The CIS has also published a companion document that provides a number of security metrics for each control [CIS15]. Each metric includes a set of three risk threshold values (lower, moderate, higher). The risk

https://t.me/learningnets

threshold values reflect the consensus of experienced practitioners. They are offered as a way for adopters of the controls to think about and choose metrics in the context of their own security improvement programs.

For example, Table 18.4 shows the metrics defined for the Maintenance, Monitoring, and Analysis of Audit Logs control.

TABLE 18.4 Metrics for the CIS Maintenance, Monitoring, and Analysis of Audit Logs Control

Metric	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
What percentage of the organization's systems do not currently have comprehensive logging enabled in accordance with the organization's standard (by business unit)?	Less than 1%	1%–4%	5%–10%
What percentage of the organization's systems are not currently configured to centralize their logs to a central log management system (by business unit)?	Less than 1%	1%–4%	5%–10%
How many anomalies/events of interest have been discovered in the organization's logs recently (by business unit)?	—	—	—
If a system fails to log properly, how long does it take for an alert about the failure to be sent (time in minutes, by business unit)?	60 minutes	1 day	1 week
If a system fails to log properly, how long does it take for enterprise personnel to respond to the failure (time in minutes, by business unit)?	60 minutes	1 day	1 week

Information Security Metric Development Process

Figure 18.2, from SP 800-55, illustrates the process of developing information security metrics. It shows how this process takes place within a larger organizational context and demonstrates that information security metrics are used to progressively measure implementation, efficiency, effectiveness, and the business impact of information security activities within organizations or for specific systems.

https://t.me/learningnets

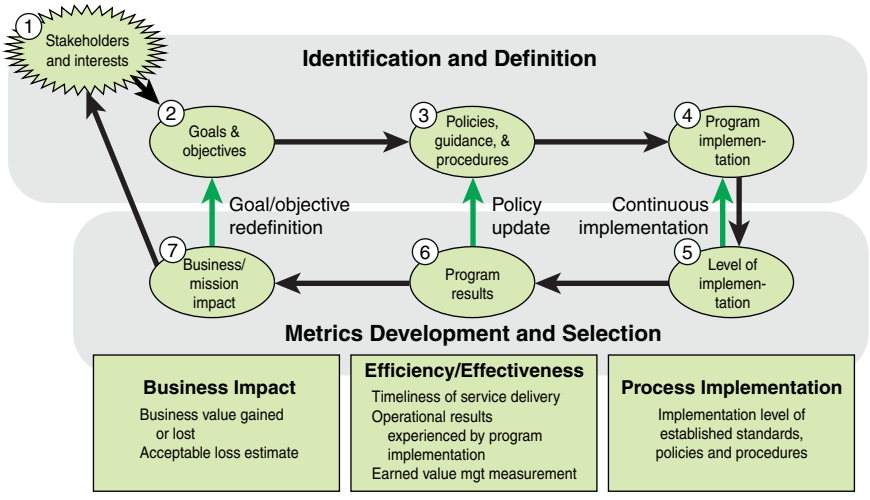


FIGURE 18.2 Information Security Metrics Development Process

The information security metric development process consists of two major activities:

1. Identifying and defining the current information security program
2. Developing and selecting specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls

The first four phases shown in Figure 18.2 summarize the information security program development process discussed earlier in this book. Based on inputs from stakeholders and other interests, security goals and objectives are developed. The goals and objectives lead to the development of security policies, which in turn guide security program implementation.

Phases 5, 6, and 7 in Figure 18.2 involve developing metrics that measure process implementation, effectiveness and efficiency, and mission impact. The organization selects metrics that measure performance, identify causes of unsatisfactory performance, and identify areas for improvement. The metrics also provide guidance for the security manager to facilitate consistent policy implementation, effect information security policy changes, and refine goals and objectives.

Figure 18.2 shows the manner in which the development of a set of metrics interacts with the system program development process. Payne's "A Guide to Security Metrics" [PAYN06] provides guidance on implementing a metrics program consisting of the following steps:

1. **Define the metrics program goal(s) and objectives.** For example, a goal could be expressed as "Provide metrics that clearly and simply communicate how efficiently and effectively our company is balancing security risks and

https://t.me/learningnets

preventive measures, so that investments in our security program can be appropriately sized and targeted to meet our overall security objectives."

The objectives could include the following:

- "To base the security metrics program on process improvement best practices within our company."
- "To leverage any relevant measurements currently being collected."
- "To communicate metrics in formats custom-tailored to various audiences."
- "To involve stakeholders in determining what metrics to produce."

2. **Decide which metrics to generate.** Security officials can use the guidance provided by COBIT 5, NIST, and the CIS, as described earlier.
3. **Develop strategies for generating the metrics.** These strategies should specify the source of the data, the frequency of data collection, and who is responsible for raw data accuracy, data compilation into measurements, and generation of the metric.
4. **Establish benchmarks and targets.** Benchmarking is the process of comparing one's own performance and practices against peers within the industry. An organization should compare the metric values it is achieving against industry norms to determine areas where best practices suggests that improvement in the security program is needed. For example, BitSight is one company that provides this service, enabling an organization to compare its security posture to others in their industry.
    - good information on Internet security threats, vulnerabilities, and attack statistics.
5. **Determine how the metrics will be reported.** The metrics program planner should determine the context, format, frequency, distribution method, and responsibility for reporting metrics so that the end product can be visualized early on by those who will be involved in producing the metrics and those who will be using them for decision making.
6. **Create an action plan and act on it.** The plan should detail the steps that need to be taken to launch the security metrics program, along with time tables and assignments.
7. **Establish a formal program review/refinement cycle.** The security metrics plan should include formal, regular review of the program.



BitSight
https://www.bitsighttech.com/

https://t.me/learningnets

Security Monitoring and Reporting

The objective of security monitoring and reporting is to provide each audience with a relevant, accurate, comprehensive, and coherent assessment of information security performance.

COBIT 5 provides specific guidance on security monitoring and reporting based on the three processes defined earlier in this section: performance and conformance, system of internal control, and compliance with external requirements. This subsection deals with the first two processes; the last subsection of Section 18.2 discusses the final process.

For the performance and conformance process, COBIT 5 defines the following steps:

1. **Establish a monitoring approach.** Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope, and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.
2. **Set performance and conformance targets.** Work with stakeholders to define, periodically review, update, and approve performance and conformance targets within the performance measurement system.
3. **Collect and process performance and conformance data.** Collect and process timely and accurate data aligned with enterprise approaches**.**
4. **Analyze and report performance.** Periodically review and report performance against targets, using a method that provides a succinct all-around view of IT performance and fits within the enterprise monitoring system.
5. **Ensure the implementation of corrective actions.** Assist stakeholders in identifying, initiating, and tracking corrective actions to address anomalies.

For the system of internal control process, COBIT 5 defines the following steps:

1. **Monitor internal controls.** Continuously monitor, benchmark, and improve the IT control environment and control framework to meet organizational objectives.
2. **Review business process controls effectiveness.** Review the operation of controls, including a review of monitoring and test evidence, to ensure that controls in business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous control monitoring, independent assessments, command and control centers, and network operations centers.

https://t.me/learningnets

3. **Perform control self-assessments.** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies, and contracts.
4. **Identify and report control deficiencies.** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
5. **Ensure that assurance providers are independent and qualified.** Ensure that the entities performing assurance are independent from the function, groups, or organizations in scope.
6. **Plan assurance initiatives.** Plan assurance initiatives based on enterprise objectives and strategic priorities, inherent risk, resource constraints, and sufficient knowledge of the enterprise.
7. **Scope assurance initiatives.** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
8. **Execute assurance initiatives.** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance, and internal control system residual risk.

SP 800-55 provides a view of implementing the monitoring and reporting function based on the security performance metrics, shown in Figure 18.3.

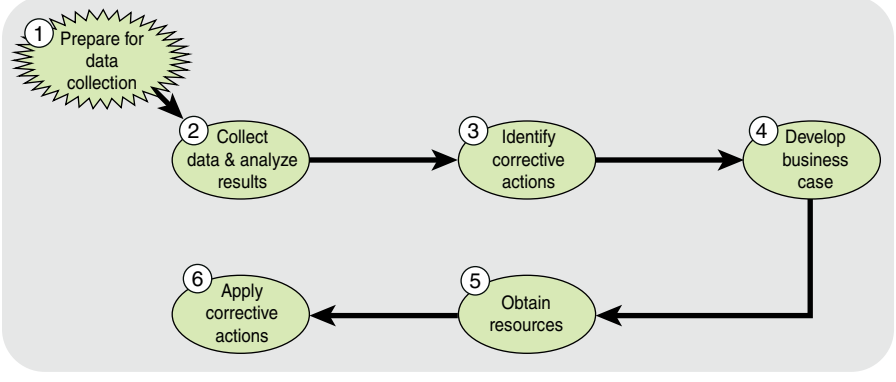


FIGURE 18.3 Information Security Metrics Program Implementation Process

https://t.me/learningnets

This process proceeds in six steps:

1. **Prepare for data collection.** In essence, this step involves the metrics development process shown in Figure 18.2.
2. **Collect data and analyze results.** The analysis should identify gaps between actual and desired performance, identify reasons for undesired results, and identify areas that require improvement.
3. **Identify corrective actions.** Based on step 2, determine appropriate corrective actions and prioritize them based on risk mitigation goals.
4. **Develop business case.** This involves developing a cost model for each corrective action and making a business case for taking that action.
5. **Obtain resources.** Obtain the needed budget and resource allocation.
6. **Apply corrective actions.** These actions may include adjustments in management, technical, and operational areas.

Information Risk Reporting

Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting describes any information security events that the institution faces and the effectiveness of management's response to and resilience in the face of those events. An organization needs to have a method of disseminating those reports to appropriate members of management. The contents of the reports should prompt action, if necessary, in a timely manner to maintain appropriate levels of risk.

One objective of information risk reporting is to provide executive management with an accurate, comprehensive, and coherent view of information risk across the organization. The second objective is to obtain approval from executive management for risk treatment options.

The Information Systems Audit and Control Association (ISACA) has developed useful guidance on information risk reporting, based on COBIT 5 [ISAC09]. The guidance makes use of two key concepts in COBIT 5:

- **Process:** A collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs, and produces outputs (for example, products, services). Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.

https://t.me/learningnets

- **Activity:** The main action taken to operate the process, which provides guidance to achieve management practices for successful governance and management of enterprise IT. Activities:
  - Describe a set of necessary and sufficient action-oriented implementation steps to achieve a governance practice or management practice
  - Consider the inputs and outputs of the process
  - Are based on generally accepted standards and good practices
  - Support establishment of clear roles and responsibilities
  - Are nonprescriptive and need to be adapted and developed into specific procedures appropriate for the enterprise

Using these concepts, ISACA outlines the goals and metrics for processes and activities that contribute to the risk reporting function, as well as the risk reporting function itself (see Table 18.5).

TABLE 18.5 Risk Reporting Goals and Metrics

Category	Goals	Metrics
Process	■ Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response	■ Percentage of risk issues inappropriately distributed too high or too low in the enterprise hierarchy ■ Number of IT-related events with business impact not earlier reported as in IT risk ■ Percentage of critical assets/resources covered by monitoring activities ■ Timeliness of reports on IT exposures relative to the next expected threat or loss event. ■ Potential business impact of exposures discovered by assurance groups
Activity	■ Communicate IT risk analysis results ■ Report IT risk management activities and state of compliance ■ Interpret independent IT assessment findings	■ Percentage of risk analysis reports accepted on initial delivery ■ Percentage of on-time risk management reports ■ Frequency of risk management activity reporting ■ Number of IT-related events with business impact not previously reported as an IT risk. ■ Number of IT risk issues identified by outside parties yet to be interpreted and mapped into the risk profile
Risk reporting	■ Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities	■ The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

https://t.me/learningnets

Information Security Compliance Monitoring

The objective of information security compliance monitoring is to ensure that information security controls are consistently prioritized and addressed according to information security obligations associated with legislation, regulations, contracts, industry standards, or organizational policies.

COBIT 5 Guidelines

COBIT 5 provides specific guidance on security monitoring and reporting for compliance with external requirements.

For the process of ensuring compliance with external requirements, COBIT 5 defines the following steps:

1. **Identify external compliance requirements.** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that the organization must comply with from an IT perspective.
2. **Optimize response to external requirements.** Review and adjust policies, principles, standards, procedures, and methodologies to ensure that legal, regulatory, and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and good practice guidance for adoption and adaptation.
3. **Confirm external compliance.** Confirm compliance of policies, principles, standards, procedures, and methodologies with legal, regulatory, and contractual requirements.
4. **Obtain assurance of external compliance.** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures, and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

Compliance Strategy

The following steps constitute a general approach to information security compliance monitoring:

1. Identify key stakeholders and/or partners across the organization who regularly deal with institutional compliance issues (for example, legal, risk management, privacy, audit).
2. Identify key standards, regulations, contractual commitments, and other areas that address specific requirements for security and privacy.

https://t.me/learningnets

3. Perform a high-level gap analysis of each compliance requirement that is applicable to determine where progress needs to be made.
4. Develop a prioritized action plan that will help organize remedial efforts.
5. Develop a compliance policy, standard, roles and responsibilities, and/or procedures in collaboration with other key stakeholders.

18.3 Security Monitoring and Improvement Best Practices

The SGP breaks down the best practices in the security monitoring and improvement category into two areas and eight topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Security audit:** This area provides guidance for conducting thorough, independent, and regular audits of the security status of target environments (critical business environments, processes, applications, and supporting systems/networks).
- **Security audit management:** The objective of this topic is to ensure that security controls have been implemented effectively and that risk is being adequately managed and to provide the owners of target environments and executive management with an independent assessment of their security status.
  - **Security audit process—planning:** Provides guidance on a methodology for security audits.
  - **Security audit process—fieldwork:** Provides a checklist of actions related to collecting relevant background material, performing security audit tests, and recording the results of the tests.
  - **Security audit process—reporting:** Provides a checklist of items that should be in the security audit report, as well as guidance on the reporting process.
  - **Security audit process—monitoring:** Provides a checklist of actions to ensure the risks identified during security audits are treated effectively, compliance requirements are being met, and agreed security controls are being implemented within agreed time scales.
- **Security performance:** This area provides guidance for monitoring information risks; compliance with the security-related elements of legal, regulatory, and contractual requirements; and the overall information security condition of the organization on a regular basis, reporting the results to specific audiences, such as executive management.

https://t.me/learningnets

- **Security monitoring and performance:** The objective of this topic is to ensure that there is a reporting function that provides selected audiences with a relevant, accurate, comprehensive, and coherent assessment of information security performance.
- **Information risk reporting:** The objective of this topic is to ensure that there is a reporting function that provides executive management with an accurate, comprehensive, and coherent view of information risk across the organization.
- **Information security compliance monitoring:** This topic provides guidelines for a security management process that should be established, which comprises information security controls derived from regulatory and legal drivers and contracts.

18.4 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms.

activity
alarm processor
archive
audit analyzer
audit archiver
audit provider
audit recorder
audit trail
audit trail examiner
event discriminator
external security audit
internal security audit
process
security audit
security audit control
security audit trail
security performance
security performance metric
security report

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

1. Briefly define the terms *security audit* and *security audit trail*.
2. What are the key elements of the X.816 security audit model's relationship with security alarms?
3. What are some of the auditable items suggested in the X.816 model of security audits and alarms?
4. What are the four different types of audit trails?

https://t.me/learningnets

5. What are the key objectives of an external security audit?
6. How does the SGP define the security performance function?
7. NIST IR 7564 defines three broad uses of security metrics. Enumerate them.
8. What are the three key processes for the COBIT 5 Monitor, Evaluate, and Assess domain?
9. What guidelines does COBIT 5 define for the performance and conformance process?
10. Describe the monitoring and reporting function, as per SP 800-55.
11. ISACA's guidance on information risk reporting is based on which two concepts of COBIT 5?
12. What are the generic steps for security compliance monitoring?

18.5 References

CIS15: Center for Internet Security. *A Measurement Companion to the CIS Critical Security Controls*. October 2015. https://www.cisecurity.org/white-papers/a-measurement-companion-to-the-cis-critical-controls/

ISAC09: ISACA, *The Risk IT Framework*. 2009. www.isaca.org

PAYN06: Payne, S., "A Guide to Security Metrics." *SANS Institute White Paper*. June 19, 2006. https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

YEE17: Yee, G., "Security Metrics: An Introduction and Literature Review." In Vacca, J. (Ed.), *Computer and Information Security Handbook*. Cambridge MA: Elsevier, 2017.

https://t.me/learningnets

Appendix A

References and Standards

In matters of this kind, everyone feels he is justified in writing and publishing the first thing that comes into his head when he picks up a pen, and thinks his own idea as axiomatic as the fact that two and two make four. If critics would go to the trouble of thinking about the subject for years on end and testing each conclusion against the actual history of war, as I have done, they would undoubtedly be more careful of what they wrote...

—*On War*, Carl von Clausewitz

References

The references listed here is a compilation of the references cited within the chapters.

ARMY10: Department of the Army. *Physical Security.* Field Manual FM 3-99.32, August 2010.

ASHO17: Ashok, I. "Hackers spied and stole from millions by exploiting Word flaw as Microsoft probed bug for months." *International Business Times*, April 27, 2017.

BALA15: Balasubramanian, V. *Conquering the Operational Challenges of Network Change & Configuration Management through Automation.* Zoho Corp. White Paper, 2015. https://www.manageengine.com/network-configuration-manager/network-configuration-management-overview.html

BANK14: Banks, E. "Automating Network Device Configuration." *Network World*, July 2014.

BAYL13: Baylor, K. "Top 8 DRM Best Practices." NSS Labs Research Report. 2013. https://www.nsslabs.com/linkservid/A59EC3DC-5056-9046-9336E175181E14C9/

BEHL12: Behl, A. *Securing Cisco IP Telephony Networks.* Indianapolis, IN: Cisco Press, 2012.

BELL94: Bellovin, S., and Cheswick, W. "Network Firewalls." *IEEE Communications Magazine*, September 1994.

https://t.me/learningnets

BEUC09: Buecker, A., Andreas, P., & Paisley, S., *Understanding IT Perimeter Security*. IBM red paper REDP-4397-00, November 2009.

BONN12: Bonneau, J. "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords." *IEEE Symposium on Security and Privacy*, 2012.

BOSW14: Bosworth, S.; Kabay, M.; and Whyne, E., Editors. *Computer Security Handbook.* New York: Wiley, 2014.

BSA03: Business Software Alliance. *Information Security Governance: Toward a Framework for Action.* 2003. https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf

BUEC09: Buecker, A.; Andreas, P.; and Paisley, S. Understanding IT Perimeter Security. IBM Redpaper REDP-4397-00, November 2009.

BURK12: Burkett, J. "Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA." *Information Security Journal*, February 15, 2012

BURN15: Burnett, M. "Today I Am Releasing Ten Million Passwords." February 9, 2015. https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495

CARB17: Carbon Black. *Beyond the Hype: Security Experts Weigh in on Artificial Intelligence, Machine Learning and Non-malware Attacks.* March 2017 https://www.carbonblack.com/wp-content/uploads/2017/03/Carbon_Black_Research_Report_NonMalwareAttacks_ArtificialIntelligence_MachineLearning_BeyondtheHype.pdf

CIS15: Center for Internet Security. *A Measurement Companion to the CIS Critical Security Controls.* October 2015. https://www.cisecurity.org/white-papers/a-measurement-companion-to-the-cis-critical-controls/

CIS18: Center for Internet Security. *The CIS Critical Security Controls for Effective Cyber Defense version 7.* 2018. https://www.cisecurity.org/controls/

CSCC15: Cloud Standards Customer Council. *Practical Guide to Cloud Service Agreements.* April 2015. http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

CSCC16: Cloud Standards Customer Council. *Public Cloud Service Agreements: What to Expect and What to Negotiate.* August 2016. http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf

CEB15: CEB/Gartner. *Information Security Strategy on a Page.* 2015. https://www.cebglobal.com/information-technology/it-risk/information-security-strategic-plan.html

CGTF04: Corporate Governance Task Force. *Information Security Governance: A Call to Action.* U.S. Department of Homeland Security, 2004.

CHES17: Chesla, A. "Restoring Machine Learning's Good Name in Cybersecurity." Forbes Community Voice, July 25, 2017. https://www.forbes.com/sites/forbestechcouncil/2017/07/25/restoring-machine-learnings-good-name-in-cybersecurity/#18be0e1168f4

https://t.me/learningnets

CICE14: Cicerone, R., and Nurse, P., Editors. *Cybersecurity Dilemmas: Technology, Policy, and Incentives.* National Academy of Sciences, 2014.

CISC07: Cisco Systems. *Cisco Advanced Services Network Management Systems Architectural Leading Practice.* White Paper C07-400447-00, September 2007. https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb4c.pdf

CIS09: Center for Internet Security. *Security Benchmark for Multi-Function Devices.* April 2009. https://www.cisecurity.org

CIS18: Center for Internet Security. *CIS Controls Version 7.* 2018. https://www.cisecurity.org

CLAR14: Clark, D.; Berson, T.'; and Lin, H., Editors. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* National Research Council, 2014.

CLEE09: van Cleeff, A.; Pieters, W.; and Wieringa, R. "Security Implications of Virtualization: A Literature Study." *International Conference on Computational Science and Engineering*, IEEE, 2009.

CMU03: Carnegie-Mellon University. *Handbook for Computer Security Incident Response Teams (CSIRTs).* CMU Handbook CMU/SEI-2004-HB-002, 2003.

CNSS10: Committee on National Security Systems. *National Information Assurance (IA) Glossary.* April 2010.

COCS14: Council on CyberSecurity. *Cybersecurity Workforce Handbook: A Practical Guide to Managing Your Workforce.* 2014. http://pellcenter.org/tag/council-on-cybersecurity/

COGE16: Cogent Communications, Inc. Network Services Service Level Agreement Global. September 2016. http://www.cogentco.com/files/docs/network/performance/global_sla.pdf

CREN17: Crenshaw, A. "Hacking Network Printers." Retrieved June 26, 2017 from http://www.irongeek.com/i.php?page=security/networkprinterhacking

DHS10: U.S. Department of Homeland Security and the U.K. Centre for the Protection of National Infrastructure. *Cyber Security Assessments of Industrial Control Systems.* November 2010.

DHS11: U.S. Department of Homeland Security. *Catalog of Control Systems Security: Recommendations for Standards Developers.* Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, April 2011.

DHS15: U.S. Department of Homeland Security. *Seven Steps to Effectively Defend Industrial Control Systems*. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, December 2015.

DHS16: U.S. Department of Homeland Security. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, September 2016.

https://t.me/learningnets

DHS17: U.S. Department of Homeland Security. *Study on Mobile Device Security*. DHS Report, April 2017.

EAPA17: The EA Pad. "Basic Elements of Federal Enterprise Architecture." https://eapad.dk/gov/us/common-approach/basic-elements-of-federal-enterprise-architecture/ retrieved April 15, 2017.

ENGE14: Engel, G. "Deconstructing the Cyber Kill Chain." DarkReading, November 18, 2014. http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

ENIS07: European Union Agency for Network and Information Security. *Information Security Awareness Initiatives: Current Practice and the Measurement of Success.* July 2008. https://www.enisa.europa.eu

ENIS08: European Union Agency for Network and Information Security. *The New Users' Guide: How to Raise Information Security Awareness.* July 2008 https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

ENIS10: European Union Agency for Network and Information Security. *ENISA IT Business Continuity Management: An Approach for Small and Medium Sized Organizations.* January 2010. https://www.enisa.europa.eu/publications/business-continuity-for-smes/at_download/fullReport

ENIS14: European Union Agency for Network and Information Security. *Algorithms, Key Size and Parameters—2014*. November 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

ENIS16: European Union Agency for Network and Information Security. *ENISA Threat Taxonomy—A Tool for Structuring Threat Information.* January 2016. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

ENIS18: European Union Agency for Network and Information Security. *ENISA Threat Landscape Report 2017.* January 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

EO13: Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." *Federal Register*, February 19, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

FEMA09: Federal Emergency Management Agency. *Continuity Guidance for Non-Federal Entities (States, Territories, Tribal and Local Government Jurisdictions, and Private Sector Organizations).* Continuity Guidance Circular 1 (CGC 1), January 21, 2009.

FFIE02: Federal Financial Institutions Examination Council. *Information Security.* December 2002.

FFIE15: Federal Financial Institutions Examination Council. *Business Continuity Planning.* February 2015.

FIRS15: First.org, Inc. *Common Vulnerability Scoring System v3.0: Specification Document.* 2015.

https://t.me/learningnets

GADS06: Gadsden, R. *MUSC Information Security Guidelines: Risk Management.* Medical University of South Carolina, 2006. https://mainweb-v.musc.edu/security/guidelines/

GAO04: Government Accountability Office. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity.* GAO-04-394G, March 2004.

GAO12: United States Government Accountability Office. *Portfolio Management Approach Needed to Improve Major Acquisition Outcomes.* GAO-12-918, September 2012.

GARR10: Garretson, C. "Pulling the Plug on Old Hardware: Life-Cycle Management Explained." *ComputerWorld*, April 22, 2010.

GOBL02: Goble, G.; Fields, H.; and Cocchiara, R. *Resilient Infrastructure: Improving Your Business Resilience.* IBM Global Service White Paper. September 2002.

GOOD12: Goodin, D. "Why Passwords Have Never Been Weaker—and Crackers Have Never Been Stronger." *Ars Technica*, August 20, 2012.

GOUL15: Gould, L. "Introducing Application Lifecycle Management." *Automotive Design and Production Magazine*, November 2015.

GRAH12: Graham-Rowe, D. "Ageing Eyes Hinder Biometric Scans." *Nature*, May 2, 2012.

HABI17: Habib, H., et al. "Password Creation in the Presence of Blacklists." 2017 Workshop on Usable Security (USEC '17), 2017.

HAYD08a: Haydamack, C. "Strategic Planning Processes for Information Technology." *BPTrends*, September 2008

HAYD08b: Haydamack, C., and Sarah Johnson. *Aligning IT with Business Goals through Strategic Planning.* Intel Information Technology White Paper, December 2008.

HEIS14a: Higher Education Information Security Council. "Records Retention and Disposition Toolkit." *Information Security Guide*, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Records+Retention+and+Disposition+Toolkit

HEIS14b: Higher Education Information Security Council. "Cloud Computing Security." *Information Security Guide*, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Cloud+Computing+Security

HEIS14c: Higher Education Information Security Council. "Identity and Access Management." *Information Security Guide*, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Identity+and+Access+Management

HERL12: Herley, C., and Oorschot, P. "A Research Agenda Acknowledging the Persistence of Passwords." *IEEE Security&Privacy*, January/February 2012.

HERN06: Hernan, S.; Lambert, S.; Ostwald, T.; and Shostack, A. "Uncover Security Design Flaws Using The STRIDE Approach." *MSDN Magazine*, November 2006.

https://t.me/learningnets

HIRT15: Hirt, R. "Review of Enterprise Security Risk Management." Slideshare, 2015. https://www.slideshare.net/randhirt/review-of-enterprise-security-risk-management

HUTT07: Hutton, N. "Preparing for Security Event Management." 360is Blog, February 28, 2017. http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf

IAIT12: The International Association of Information Technology Asset Managers. *What is IT Asset Management?* White Paper, 2012.

IFIT09: The International Foundation for Information Technology. *System Development Management*. 2009 https://www.if4it.com/SYNTHESIZED/DISCIPLINES/System_Development_Management_Home_Page.html

IBM14: IBM. "IBM Predictive Maintenance and Quality (Version 2.0)." IBM Redbooks Solution Guide, 2014.

INFO14: INFOSEC Institute. *Information Security Policies.* April 16, 2014. http://resources.infosecinstitute.com/information-security-policies/

ISAC08: ISACA. *Defining Information Security Management Position Requirements: Guidance for Executives and Managers.* 2008. www.isaca.org

ISAC09: ISACA. *The Risk IT Framework.* 2009. www.isaca.org

ISAC10: ISACA. *Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives.* 2008. www.isaca.org

ISAC11: ISACA. *Creating a Culture of Security.* 2011. www.isaca.org

ISAC13: ISACA. *Responding to Targeted Cyberattacks.* 2008. www.isaca.org

ITGI06: IT Governance Institute. *Information Security Governance Guidance for Boards of Directors and Executive Management.* 2006. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

ITUT12: ITU-T. *Focus Group on Cloud Computing Technical Report Part 5: Cloud Security.* FG Cloud TR, February 2012.

ITUT15: ITU-T. *Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of existing ITU-T Recommendations for Secure Telecommunications.* September 2015.

JOHN09: Johnston, A., and Hale, R. "Improved Security through Information Security Governance." *Communications of the ACM*, January 2009.

JUDY14: Judy, H., et al. "Privacy in Cyberspace." In [BOSW14].

JUER13: Juergens, M.; Donohue, T.; and Smith, C. "End-User Computing: Solving the Problem." *CompAct*, April 2013. https://www.soa.org/News-and-Publications/Newsletters/Compact/2013/april/End-User-Computing--Solving-the-Problem.aspx

https://t.me/learningnets

JUIZ15: Juiz, C., and Toomey, M. "To Govern IT, or not to Govern IT?" *Communications of the ACM*, February 2015.

KABA14: Kabay, M., and Robertson, B. "Employment Practices and Policies." In [BOSW14].

KEIZ17: Keizer, G. "Experts Contend Microsoft Canceled Feb. Updates to Patch NSA Exploits." *ComputerWorld*, April 18, 2017.

KELL12: Kelley, P., et al. "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms." *IEEE Symposium on Security and Privacy*, 2012

KENN03: Kennedy, S. "Best Practices for Wireless Network Security." *ComputerWorld*, November 23, 2003.

KINA16: Kinast, K. "10 key facts businesses need to note about the GDPR." European Identity & Cloud Conference, 2016.

KOMA11: Komanduri, S. "Of Passwords and People: Measuring the Effect of Password-Composition Policies." *CHI Conference on Human Factors in Computing Systems*, 2011.

KOWA12: Kowall, J., and Cappelli, W. *Magic Quadrant for Application Performance Monitoring.* Gartner Report, 2013. https://www.gartner.com/doc/2125315/magic-quadrant-application-performance-monitoring

LAMB06: Lambo, T. "ISO/IEC 27001: The Future of Infosec Certification." *ISSA Journal*, November 2006.

MAAW10: Messaging Anti-Abuse Working Group. *Overview of DNS Security - Port 53 Protection.* MAAWG Paper, June 2010. https://www.m3aawg.org

MAZU13: Mazurek, M., et al. "Measuring Password Guessability for an Entire University." *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, November 2013.

MCFA83: McFarlan, F. "The Information Archipelago—Plotting a Course." *Harvard Business Review*, January 1983.

MICR15: Microsoft. *Enterprise DevOps.* Microsoft White Paper, 2015.

MILL17: Millet, L.; Fischhoff, B.; and Weinberger, P., Editors. *Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions.* National Academies of Sciences, Engineering, and Medicine, 2017.

MINI14: Minick, E.; Rezabek, J.; and Ring, C. *Application Release and Deployment for Dummies.* Hoboken, NJ: Wiley, 2014.

MOGU07: Mogull, R. *Understanding and Selecting a Data Loss Prevention Solution*. SANS Institute White Paper, December 3, 2007. https://securosis.com/assets/library/publications/DLP-Whitepaper.pdf

https://t.me/learningnets

MOOR06: Moore, D., et al. "Inferring Internet Denial-of-Service Activity." *ACM Transactions on Computer Systems*, May, 2006.

MOUL11: Moulds, R. *Key Management for Dummies.* Hoboken, NJ: Wiley, 2011.

MYER13: Myers, L. "The practicality of the Cyber Kill Chain approach to security." CSO, October 4, 2013. https://www.cio.com/article/2381947/security0/the-practicality-of-the-cyber-kill-chain-approach-to-security.html

NAYL09: Naylor, J. *Acceptable Use Policies—Why, What, and How*. MessageLabs White Paper, 2009. http://esafety.ccceducation.org/upload/file/Policy/AUP%20Legal%20advice.pdf

NCEM12: National Emergency Crisis and Disasters Management Authority. Business Continuity Management Standard and Guide. United Arab Emirates Supreme Council for National Security Standard AE/HSC/NCEMA 7000, 2012. https://www.ncema.gov.ae/content/documents/BCM%20English%20NCEMA_29_8_2013.pdf

NILE15: Niles, S. *Physical Security in Mission Critical Facilities.* White Paper 82. Schneider Electric. March 2015. http://it-resource.schneider-electric.com/h/i/55734850-wp-82-physical-security-in-mission-critical-facilities

NIST15: NIST. *Measuring Strength of Authentication.* December 16, 2015. https://www.nist.gov/sites/default/files/nstic-strength-authentication-discussion-draft.pdf

NIST17: NIST. *Strength of Function for Authenticators – Biometrics (SOFA-B): Discussion Draft Open for Comments.* November 14, 2017. https://pages.nist.gov/SOFA/SOFA.html

NIST18: NIST. *Framework for Improving Critical Infrastructure Cybersecurity.* April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NSTC11: National Science and Technology Council. *The National Biometrics Challenge.* September 2011.

OECH03: Oechslin, P. "Making a Faster Cryptanalytic Time-Memory Trade-Off." *Proceedings, Crypto 03*, 2003.

OHKI09: Ohki, E., et al. "Information Security Governance Framework." *First ACM Workshop on Information Security Governance* (WISG), November 2009.

OMB10: Office of Management and Budget; NIST; and Federal Chief Information Officers Council. *Federal Enterprise Architecture Security and Privacy Profile.* 2010.

OMB13: Office of Management and Budget, and Federal Chief Information Officers Council. *Federal Enterprise Architecture Framework.* 2013.

OPEN15: Openwall.com. *John the Ripper Password Cracker.* http://www.openwall.com/john/doc/

OWAS17: The OWASP Foundation. OWASP Top 10 2017: The Ten Most Critical Web Application Security Risks. 2017 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

https://t.me/learningnets

PAYN06: Payne, S. *A Guide to Security Metrics*. SANS Institute White Paper. June 19, 2006. https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

PETE12: Peters, C., and Schuman, B. *Achieving Intel's Strategic Goals with IT.* Intel Information Technology White Paper, February 2012.

POLL12: Poller, A., et al., "Electronic Identity Cards for User Authentication—Promise and Practice." *IEEE Security & Privacy*, January/February 2012.

RATH01: Ratha, N.; Connell, J.; and Bolle, R. "Enhancing security and privacy in biometrics-based authentication systems." *IBM Systems Journal*, Vol 30, No 3, 2001.

RITC13: Ritchie, S. "Security Risk Management." ISACA document, August 20, 2013. http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Security%20Risk%20Management.pdf

ROE10: Roe, D. "6 Ways Document Management and Records Management Differ." *CMS Wire*, January 25, 2010.

ROY15: Roy, A., et al. "Secure the Cloud: From the Perspective of a Service-Oriented Organization." *ACM Computing Surveys*, February 2015.

RUBE14: Rubenking, N. "Trustwave Global Security Report Is Bursting with Valuable Data." *PCMag*, May 22, 2014.

SADO03: Sadowsky, G. et al. *Information Technology Security Handbook.* Washington, DC: The World Bank, 2003 http://www.infodev.org/articles/information-technology-security-handbook

SCHN14: Schneier, B. "The Internet of Things is Wildly Insecure—and Often Unpatchable." *Wired*, January 6, 2014.

SCOT07: Scott, C. "Auditing and Securing Multifunction Devices." *SANS Institute*, January 25, 2007.

SESS07: Sessions, R. "A Comparison of the Top Four Enterprise-Architecture Methodologies." Microsoft Developer Network, May 2007. http://www3.cis.gsu.edu/dtruex/courses/CIS8090/2013Articles/A%20Comparison%20of%20the%20Top%20Four%20Enterprise-Architecture%20Methodologies.html

SGM17: Strategic Management Group. *Strategic Planning Basics.* http://www.strategymanage.com/strategic-planning-basics/ retrieved April 6, 2017.

SHAR15: Sharma, S., and Coyne. B. *DevOps for Dummies.* Hoboken, NJ: Wiley, 2015.

SHER09: Sherwood, J.; Clark, A.; and Lynas, D. *Enterprise Security Architecture*. *SABSA White Paper*, 2009. http://www.sabsa.org

SHOR10: Shore, M., and Deng, X. "Architecting Survivable Networks using SABSA." *6th International Conference on Wireless Communications Networking and Mobile Computing*, 2010.

https://t.me/learningnets

SOLO06: Solove, D. *A Taxonomy of Privacy.* GWU Law School Public Law Research Paper No. 129, 2006. http://scholarship.law.gwu.edu/faculty_publications/921/

SPRA95: Sprague, R. "Electronic Document Management: Challenges and Opportunities for Information Systems Managers." *MIS Quarterly*, March 1995.

STAL16: Stallings, W. "Comprehensive Internet Email Security." *Internet Protocol Journal*, November 2016. Available at http://williamstallings.com/Papers/

STAL17: Stallings, W. *Cryptography and Network Security: Principles and Practice, Seventh Edition.* Upper Saddle River, NJ: Pearson, 2017.

STAL18: Stallings, W., and Brown, L. *Computer Security: Principles and Practice.* Englewood Cliffs, NJ: 2018.

TIMM10: Timmer, J., "32 Million Passwords Show Most Users Careless About Security." *Ars Technica*, January 21, 2010.

TOG11: The Open Group. *The Open Group Architecture Framework (TOGAF).* 2011. http://www.opengroup.org/subjectareas/enterprise/togaf

VERA17: Veracode. *State of Software Security 2017.* 2017 https://info.veracode.com/report-state-of-software-security.html

VERI17: Verizon. *2017 Data Breach Investigations Report.* 2017. http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

WAG15: Western Australian Government. Business Continuity Management Guidelines. June 2015. https://www.icwa.wa.gov.au/__data/assets/pdf_file/0010/6112/Business-Continuity-Management-Guidelines.pdf

WAGN00: Wagner, D., & Goldberg, I., "Proofs of Security for the UNIX Password Hashing Algorithm." *Proceedings, ASIACRYPT '00*, 2000.

WASC10: Web Application Security Consortium. *WASC Threat Classification*. January 2010. http://www.webappsec.org/

WEIR09: Weir, M., et al., "Password Cracking Using Probabilistic Context-Free Grammars." *IEEE Symposium on Security and Privacy*, 2009.

WEIR10: Weir, M., et al. "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords." *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 2010.

WILD13: Wilding, R. "Classification of the Sources of Supply Chain Risk and Vulnerability." Richard Wilding Blog, August 2013. http://www.richardwilding.info/blog/the-sources-of-supply-chain-risk

YEE17: Yee, G. "Security Metrics: An Introduction and Literature Review." *Computer and Information Security Handbook*. Vacca, J., ed. Cambridge MA: Elsevier. 2017.

https://t.me/learningnets

ZHAN10: Zhang, Y., Monrose, F., & Reiter, M., "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis." *ACM Conference on Computer and Communications Security*, 2010.

ZIA15: Zia, T. "Organisations Capability and Aptitude towards IT Security Governance." *2015 5th International Conference on IT Convergence and Security (ICITCS)*, August 2015.

ZIND17: Zindel, A. "IAM Best Practices to Reduce Your Attack Surface." *Centrify Blog*, August 30, 2017. https://blog.centrify.com/reduce-attack-surface-iam/

https://t.me/learningnets

List of NIST, ITU-T, and ISO Documents Referenced in the Book

NIST Documents

FIPS-140-2	*Security Requirements for Cryptographic Modules*, May 2001
FIPS-140-2A	*Approved Security Functions for FIPS PUB 140-2*, January 2018
FIPS-186	*Digital Signature Standard*, July 2013
FIPS-199	*Standards for Security Categorization of Federal Information and Information Systems*, February 2004
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*, March 2006
IR 7359	*Information Security Guide for Government Executives*, January 2007
IR 7564	*Directions in Security Metrics Research*, April 2009
IR 7621	*Small Business Information Security: The Fundamentals*, November 2016
IR 7622	*Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012
IR 7874	*Guidelines for Access Control System Evaluation Metrics*, September 2012
IR 7946	*CVSS Implementation Guidance*, April 2014
IR 7956	*Cryptographic Key Management Issues & Challenges in Cloud Services*, September 2013
IR 8023	*Risk Management for Replication Devices*, February 2015
IR 8112	*Attribute Metadata*, August 2016
IR 8144	*Assessing Threats to Mobile Devices & Infrastructure*, September 2016
IR 8062	*An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017
SP 800-12	*Introduction to Information Security*, January 2017
SP 800-16	*A Role-Based Model for Federal Information Technology/Cybersecurity Training*, March 2014
SP 800-18	*Guide for Developing Security Plans for Federal Information Systems*, February 2006
SP 800-27	*Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004
SP 800-30	*Guide for Conducting Risk Assessments*, September 2012
SP 800-32	*Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001
SP 800-34	*Contingency Planning Guide for Federal Information Systems*, May 2010
SP 800-37	*Risk Management Framework for Information Systems and Organizations*, September 2017
SP 800-39	*Managing Information Security Risk*, March 2011
SP 800-40	*Guide to Enterprise Patch Management Technologies*, July 2013
SP 800-41	*Guidelines on Firewalls and Firewall Policy*, September 2009
SP 800-45	*Guidelines on Electronic Mail Security*, February 2007

https://t.me/learningnets

SP 800-50	*Building an Information Technology Security Awareness and Training Program*, October 2003
SP 800-53	*Security and Privacy Controls for Federal Information Systems and Organizations*, August 2017
SP 800-53A	*Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014
SP 800-55	*Performance Measurement Guide for Information Security*, July 2008
SP 800-57	*Recommendation for Key Management—Part 1: General*, January 2016 *Recommendation for Key Management—Part 2: Best Practices for Key Management Organization*, August 2005 *Recommendation for Key Management—Part 3: Application-Specific Key Management Guidance*, January 2015
SP 800-60	*Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008 *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
SP 800-61	*Computer Security Incident Handling Guide*, August 2012
SP 800-63	*Digital Identity Guidelines*, June 2017.
SP 800-63B	*Digital Identity Guidelines—Authentication and Lifecycle Management*, June 2017.
SP 800-64	*Security Considerations in the System Development Life Cycle*, October 2008
SP 800-65	*Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005
SP 800-82	*Guide to Industrial Control Systems (ICS) Security*, May 2015
SP 800-86	*Guide to Integrating Forensic Techniques into Incident Response*, August 2006
SP 800-88	*Guidelines for Media Sanitization*, December 2014
SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015
SP 800-92	*Guide to Computer Security Log Management*, September 2006
SP 800-94	*Guide to Intrusion Detection and Prevention Systems*, February 2007
SP 800-100	*Information Security Handbook: A Guide for Managers*, October 2007
SP 800-116	*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, December 2015
SP 800-122	*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
SP 800-123	*Guide to General Server Security*, July 2008
SP 800-124	*Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013
SP 800-125	*Guide to Security for Full Virtualization Technologies*, January 2011
SP 800-125A	*Security Recommendations for Hypervisor Deployment*, September 2017
SP 800-130	*A Framework for Designing Cryptographic Key Management Systems*, August 2013
SP 800-131A	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015
SP 800-144	*Guidelines on Security and Privacy in Public Cloud Computing*, December 2011

https://t.me/learningnets

SP 800-145 *The NIST Definition of Cloud Computing*, January 2011
SP 800-146 *Cloud Computing Synopsis and Recommendations*, May 2012
SP 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015
SP 800-162 *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, January 2014
SP 800-163 *Vetting the Security of Mobile Applications*, January 2015
SP 800-164 *Guidelines on Hardware-Rooted Security in Mobile Devices*, October 2012
SP 800-177 *Trustworthy Email*, September 2017
SP 800-178 *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications*, October 2016
SP 1500-201 *Framework for Cyber-Physical Systems: Volume 1, Overview*, June 2017
SP 1500-202 *Framework for Cyber-Physical Systems: Volume 2, Working Group Reports*, June 2017
SP 1800-3 *Attribute Based Access Control*, September 2017
SP 1800-4 *Mobile Device Security: Cloud and Hybrid Builds*, November 2015

ITU-T Documents

M.3400 *Telecommunications Management Functions*, February 2000
X.816 *Security Audit and Alarms Framework*, November 1995
X.1054 *Governance of Information Security*, September 2012
X.1055 *Risk Management and Risk Profile Guidelines for Telecommunication Organizations*, November 2008
X.1056 *Security Incident Management Guidelines for Telecommunications Organizations*, January 2009
X.1205 *Overview of Cybersecurity*, April 2014

ISO Documents

7498-2 *Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*, February 1989
7498-4 *Open Systems Interconnection—Basic Reference Model—Part 4: Management Framework*, November 1989
27000 *ISMS—Overview and Vocabulary*, February 2016
27001 *ISMS—Requirements*, October 2013
27002 *Code of Practice for Information Security Controls*, October 2013
27005 *Information Security Risk Management*, June 2011
27014 *Governance of Information Security*, May 2013
27035-1 *Information Security Incident Management—Part 1: Principles of Incident Management*, November 2016
27035-2 *Information Security Incident Management—Part 2:Guidelines to Plan and Prepare for Incident Response*, November 2016
29100 *Privacy Framework*, December 2011

https://t.me/learningnets

Appendix B

Glossary

In studying the Imperium, Arrakis, and the whole culture which produced Maud'Dib, many unfamiliar terms occur. To increase understanding is a laudable goal, hence the definitions and explanations given below.

—*Dune*, Frank Herbert

acceptable use policy (AUP): A policy that defines for all parties the ranges of use that are approved for use of information, systems, and services within an organization.

access control: The process of granting or denying specific requests (1) for accessing and using information and related information processing services and (2) to enter specific physical facilities. Access control ensures that access to assets is authorized and restricted based on business and security requirements.

accidental behavior: Actions that do not involve a motive to harm or a conscious decision to act inappropriately (for example, emailing sensitive information to unauthorized recipients, opening malicious email attachments, publishing personal information on publicly available servers).

accountability: The property of a system or system resource which ensures that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.

advanced persistent threat (APT): A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry. APTs differ from other types of attack in their careful target selection and persistent, often stealthy, intrusion efforts over extended periods.

application life cycle management: The administration and control of an application from inception to demise. It embraces requirements management, system design, software development,

https://t.me/learningnets

and configuration management and implies an integrated set of tools for developing and controlling the project.

application management: The process of managing the operation, maintenance, versioning and upgrading of an application throughout its life cycle. It includes best practices, techniques, and procedures essential to a deployed application's optimal operation, performance, and efficiency throughout the enterprise and back-end IT infrastructure.

application performance management: The practice in systems management that targets managing and tracking the availability and efficiency of software applications. It involves translating IT metrics into business meaning. It examines the workflow and the associated IT tools that are deployed to analyze, identify, and report application performance concerns to make sure the expectations of businesses and end users are met. Application performance signifies how quickly transactions are accomplished or details are sent to end users of a particular application.

application portfolio management: An IT management technique that involves applying cost/benefit analysis and other business analytics to IT decision making. Application portfolio management looks at each program and piece of equipment as an asset in a company's overall portfolio and gives it a score based on factors such as age, importance, and number of users. Further investment in upgrades or changes in the portfolio mix must be justified by projected returns and other measurable factors.

application security: The use of software, hardware, and procedural methods to protect applications from external threats. Application security includes adding features or functionality to the application software to prevent a range of different threats. It also includes security features outside the application, such as firewalls, antivirus, and access control methods.

application whitelisting: The practice of specifying an index of approved software applications that are permitted to be present and active on a computer system and prevents execution of all other software on the system.

architecture: The way the component parts of an entity are arranged, organized, and managed.

asset: Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (that is, a system component—hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or information itself.

attack surface: The reachable and exploitable vulnerabilities in a system.

attribute-based access control (ABAC): Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

authentication: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

https://t.me/learningnets

authentication factor: A method of authentication, based on either something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints or other forms of biometrics).

authenticator: The means used to confirm the identity of a user, process, or device (for example, user password, token). An authentication factor is based on the use of a particular type of authenticator.

authenticity: The property of being genuine and being able to be verified and trusted. This involves verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

authorization: In the context of system access, the granting of access or other rights to a user, program, or process to access system resources. Authorization defines what an individual or program can do after successful authentication.

availability: The property of a system or a system resource being accessible or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; a system is available if it provides services according to the system design whenever users request them.

bring your own device (BYOD): An IT strategy in which employees, business partners, and other users can utilize a personally selected and purchased client device to execute enterprise applications and access data and the corporate network. Typically, it spans smartphones and tablets, but the strategy may also be used for laptops. It may include a subsidy.

business continuity: Capability of an organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business continuity embraces all the operations in a company, including how employees function in compromised situations.

business continuity management: A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and that provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

business continuity management system: Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity. The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes, and resources.

business continuity manager: An individual who manages, designs, oversees, and/or assesses an enterprise's business continuity capability to ensure that the enterprise's critical functions continue to operate following disruptive events.

business continuity plan: Documented procedures that guide organizations to respond, recover, resume, and restore to a predefined level of operation following disruption.

https://t.me/learningnets

business continuity program: An ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

business impact analysis (BIA): The analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

business resilience: The ability of an organization to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and overall brand equity. Business resilience goes a step beyond disaster recovery, by offering post-disaster strategies to avoid costly downtime, shore up vulnerabilities, and maintain business operations in the face of additional, unexpected breaches.

C-level: Chief level. Refers to high-ranking executive titles within an organization. Officers who hold C-level positions set the company's strategy, make higher-stakes decisions, and ensure that the day-to-day operations align with fulfilling the company's strategic goals.

capital planning: A decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and management of IT in support of an organization's missions and business needs.

certification: The provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements. Also known as *third-party conformity assessment*.

certification and accreditation: A comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. *Accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

change control: A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted, and that resources are used efficiently.

change control board: A committee that makes decisions regarding whether proposed changes to a system should be implemented.

change management: The process of minimizing resistance to organizational change through involvement of key players and stakeholders.

chief executive officer (CEO): The person who is ultimately responsible for the success or failure of the organization, overseeing the entire operation at a high level. The CEP is the boss of all other executives.

https://t.me/learningnets

chief information officer (CIO): The person who is in charge of information technology (IT) strategy and the computer, network, and third-party (for example, cloud) systems required to support an enterprise's objectives and goals.

chief operating officer (COO): Generally the person who is second in command to the CEO. The COO oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations.

chief privacy officer (CPO): The person who is charged with developing and implementing policies designed to protect employee and customer data from unauthorized access.

chief risk officer (CRO): The person who is charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings.

chief security officer (CSO) or chief information security officer (CISO): The person who is tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security and a CISO in charge of digital security.

commercial off the shelf (COTS): An item that is commercially available, leased, licensed, or sold to the general public and that requires no special modification or maintenance over the life cycle of the product to meet the needs of the procuring agency.

Computer Security Incident Response Team (CSIRT): An organization that receives reports of security breaches, conducts analyses of the reports, and responds to the senders.

confidentiality: The property that data is not disclosed to system entities unless they have been authorized to know the data.

configuration management: The process of controlling modifications to a system's hardware, software, and documentation, which provides sufficient assurance that the system is protected against the introduction of improper modification before, doing, and after system implementation.

configuration management database (CMDB): A database that contains all relevant information about the components of the information system (including software, hardware, and documentation) used in an organization's IT services and the relationships between those components. A CMDB provides an organized view of data and a means of examining that data from any desired perspective.

countermeasure: An action, a device, a procedure, or a technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

critical information: Information that needs to be available and have integrity (for example, product prices/exchange rates, manufacturing information, medical records).

cryptographic algorithm: An algorithm that uses the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key-agreement algorithms.

https://t.me/learningnets

cryptographic erasure: The process of encrypting all the data on a medium and then destroying the key, making recovery impossible.

cryptosystem (cryptographic system): A set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context.

cybersecurity: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users' assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyberspace environment. The general security objectives are availability; integrity, which may include authenticity and non-repudiation; and confidentiality.

cyberspace: Artifacts based on or dependent on computer and communications technology; the information that these artifacts use, store, handle, or process; and the interconnections among these various elements.

data loss prevention (DLP): A set of technologies and inspection techniques used to classify information content contained within an object—such as a file, an email, a packet, an application or a data store—while at rest (in storage), in use (during an operation), or in transit (across a network). DLP tools also have the ability to dynamically apply a policy—such as log, report, classify, relocate, tag, and encrypt—and/or apply enterprise data rights management protections.

defense in depth: A process that involves constructing a system's security architecture with layered and complementary security mechanisms and countermeasures so that if one security mechanism is defeated, one or more other mechanisms (which are "behind" or "beneath" the first mechanism) still provide protection.

demilitarized zone (DMZ): A perimeter network segment that is physically or logically between internal and external networks. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than to the entire internal network. It provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

denial of service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations.

DevOps (development operations): The tighter integration between the developers of applications and the IT department that tests and deploys them. DevOps is said to be the intersection of software engineering, quality assurance, and operations.

directory server: A server that manages user identity and authorization data in a directory format.

https://t.me/learningnets

disaster recovery (DR): An area of security planning that aims to protect an organization from the effects of significant negative events. DR allows an organization to maintain or quickly resume mission-critical functions following a disaster.

discretionary access control (DAC): Access control based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

distributed denial of service (DDoS): A DoS attack in which multiple systems are used to flood servers with traffic in an attempt to overwhelm available resources (transmission capacity, memory, processing power, and so on), making them unavailable to respond to legitimate users.

document management: The capture and management of documents in an organization. The term originally implied only the management of documents after they were scanned into the computer. Subsequently, it became an umbrella term embracing document imaging, workflow, text retrieval, and multimedia.

document management system: Software that manages documents for electronic publishing. It generally supports a large variety of document formats and provides extensive access control and searching capabilities across networks. A document management system may support multiple versions of a document and may be able to combine text fragments written by different authors. It often includes a workflow component that routes documents to the appropriate users.

enterprise architecture: The systems, infrastructure, operations, and management of all information technology throughout an enterprise. The architecture is typically organized as high-level internally compatible representations of organizational business models, data, applications, and information technology infrastructure.

enterprise strategic planning: The definition of long-term goals and objectives for an organization (for example, business enterprise, government agency, nonprofit organization) and the development of plans to achieve these goals and objectives.

environment: A particular configuration of hardware or software. The environment refers to a hardware platform and the operating system that is used in it. A programming environment would include the compiler and associated development tools. Environment is also used to express a type of configuration, such as a networking environment, database environment, transaction processing environment, batch environment, interactive environment, and so on.

event: An occurrence or a change in a particular set of circumstances.

exfiltration: A malware feature that automates the sending of harvested victim data, such as login credentials and cardholder information, back to an attacker-controlled server.

exploit: An attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders.

https://t.me/learningnets

external security audit: An audit conducted by an organization independent of the one being audited.

fault: An abnormal condition that causes a device or system component to fail to perform in a required manner and that requires management attention (or action) to repair.

forward proxy: A server that requests resources from the Internet or a remote server on behalf of one or more users on client systems. The proxy may perform protocol translations or other transformations needed between the client's software and the server application.

functional testing: Security testing in which advertised security mechanisms of an information system are tested under operational conditions to determine if a given function works according to its requirements.

golden record: A single, well-defined version of all the data entities in an organizational ecosystem. In this context, a golden record is sometimes called the "single version of the truth," where "truth" is understood to mean the reference to which data users can turn when they want to ensure that they have the correct version of a piece of information.

group key: A symmetric cryptographic key shared among multiple participants. A block of data encrypted by any one participant using the group key can be decrypted by any other participant who shares the group key.

hardware: Any physical asset that is used to support corporate information or systems (for example, a server, network device, mobile device, printer, or specialized equipment, such as that used by manufacturing, transport, or utility companies), including the software embedded within them and the operating systems supporting them.

hardware life cycle management: A subset discipline of IT asset management that deals specifically with the hardware portion of IT assets. It is the process of managing the physical components of computers, computer networks, and systems. It begins with acquisition and continues through maintenance until the hardware's ultimate disposal. Also known as *hardware asset management*.

hash value: A numerical value produced by a mathematical function, which generates a fixed-length value typically much smaller than the input to the function. The function is many to one, but generally, for all practical purposes, each file or other data block input to a hash function yields a unique hash value.

impact: An adverse change to the level of business objectives achieved. Also called *impact level* or *impact value*.

industrial control system (ICS): A system that is used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. An ICS consists of combinations of control

https://t.me/learningnets

components (for example, electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (for example, manufacturing, transportation of matter or energy).

information and communications technology (ICT): The collection of devices, networking components, applications, and systems that together allow people and organizations to interact in the digital world. ICT is sometimes used synonymously with IT; however, ICT is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

information security architecture: An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

information security governance: The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

information security implementation/operations: The management of information risk through the implementation, deployment, and ongoing operation of security controls defined within a cybersecurity framework.

information security management: The supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

information security management system (ISMS): The policies, procedures, guidelines, and associated resources and activities collectively managed by an organization in the pursuit of protecting its information assets.

information security strategic planning: The process of aligning information security management and operation with enterprise and IT strategic planning.

information system boundaries: Boundaries that establish the scope of protection for organizational information systems (that is, what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes. Also referred to as *authorization boundaries*.

information system contingency planning: Management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

https://t.me/learningnets

information system resilience: The ability of an information system to continue to (1) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover to an effective operational posture in a time frame consistent with mission needs.

information technology (IT): Applied computer systems, both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. IT is often the name of the part of an enterprise that deals with all things electronic.

information type: A specific category of information (for example, privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, directive, policy, or regulation.

inherent risk: The probability of loss arising out of circumstances or existing in an environment in the absence of any action to control or modify the circumstances.

integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

intellectual property rights (IPR): Rights to a body of knowledge, ideas, or concepts produced by an entity that is claimed by that entity to be original and of copyright-type quality.

internal security audit: An audit conducted by personnel responsible to the management of the organization being audited.

IT service management: A general term that describes a strategic approach for designing, delivering, managing, and improving the way IT is used within an organization. The goal of every IT service management framework is to ensure that the right processes, people, and technologies are in place for the organization to meet its business goals.

IT strategic planning: The alignment of IT management and operation with enterprise strategic planning**.**

key performance indicators (KPIs): Quantifiable measurements, agreed to beforehand, that reflect the critical success factors of an organization.

kill chain: A systematic process to target and engage an adversary to create desired effects. In the context of cybersecurity, it consists of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action.

least privilege: The principle that access control should be implemented so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work. This principle tends to limit damage that can be caused by an accident, an error, or a fraudulent or unauthorized act.

level of risk: The magnitude of a risk, expressed in terms of the combination of consequences and their likelihood.

https://t.me/learningnets

log: A record of the events occurring within an organization's systems and networks.

log management: The process for generating, transmitting, storing, analyzing, and disposing of log data.

malicious behavior: A combination of motive to cause harm and a conscious decision to act inappropriately (for example, copying business files before taking employment with a competitor, leaking sensitive information, misusing information for personal gain).

malicious software: Software that exploits vulnerabilities in a computing system to create an attack. Also called *malware*.

managed service provider (MSP): A company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.

maximum tolerable downtime (MTD): The duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed.

media sanitization: A process that renders access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort.

mission and business processes: What an organization does, what its perceived mission or missions are, and what business processes are involved in fulfilling the mission(s).

multifactor authentication: A process that involves using two or more factors to achieve authentication. Factors include something you know (for example, password, PIN), something you have (for example, cryptographic identification device, token), or something you are (for example, biometric).

multifunction device: A network-attached document-production device that combines two or more of the functions copy, print, scan, and fax.

negligent behavior: Action that does not involve a motive to cause harm but does involve a conscious decision to act inappropriately (for example, using unauthorized services or devices to save time, increase productivity, or enable remote working).

Network Time Protocol (NTP): A protocol that ensures accurate local timekeeping on computer systems, network devices, and other system components, with reference to radio and atomic clocks on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

non-repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

office equipment: Equipment including printers, photocopiers, facsimile machines, scanners and multifunction devices (MFDs). Office equipment often contains the same components as a server (for example, operating system, hard disk drives, network interface cards) and runs services such as web, mail, and FTP services.

https://t.me/learningnets

operational readiness: The capability of a process or equipment to perform the missions or functions for which it is organized and designed. This term may be used in a general sense or to express a level or degree of readiness.

patch management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. Patch management tasks include maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required.

penetration testing: Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, a system, or a network.

personally identifiable information (PII): Information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone or when combined with other information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

phishing: A digital form of social engineering that involves attempting to acquire sensitive data, such as bank account numbers or passwords, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

port mirror: A cross-connection of two or more ports on a network switch so that traffic can be simultaneously sent to a network analyzer or monitor connected to another port.

privacy: The right of individuals to control or influence what information related to them may be collected and stored and by whom, as well as to whom that information may be disclosed.

pseudorandom number generator: A function that deterministically produces a sequence of numbers that are apparently statistically random.

radio-frequency identification (RFID): A data collection technology that uses electronic tags attached to items to allow the items to be identified and tracked by a remote system. The tag consists of an RFID chip attached to an antenna.

records management: The creation, retention, and scheduled destruction of an organization's sensitive or important paper and electronic records. Computer-generated reports fall into the records management domain, but traditional data processing files do not.

records management system: Software that provides tools for and aids in records management.

recovery point objective (RPO): The amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (for example, the date and time of a business disruption).

recovery time objective (RTO): The target time set for resumption of product, service, or activity delivery after an incident. It is the maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions

https://t.me/learningnets

must be recovered after an outage (for example, the point in time at which a process can no longer be inoperable).

reengineering: Using information technology to improve performance and cut costs. Its main premise is to examine the goals of an organization and to redesign work and business processes from the ground up rather than simply automate existing tasks and functions.

residual risk: Risk that remains after risk treatment.

reverse proxy: A server that services requests from the Internet and makes requests to a server or application sitting behind it. Unlike with a forward proxy, with a reverse proxy, the client may not be aware that it is communicating with a reverse proxy; a reverse proxy receives requests as if it were the origin server for the target resource.

risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

risk aggregation: The process of assessing the overall risk to organizational operations, assets, and individuals, given the set of discrete risks.

risk analysis: A process undertaken to comprehend the nature of risk and to determine the level of risk.

risk assessment: The overall process of risk identification, risk analysis, and risk evaluation.

risk criteria: Terms of reference against which the significance of a risk is evaluated.

risk evaluation: The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

risk identification: The process of finding, recognizing, and describing risks.

risk management: Coordinated activities to direct and control an organization with regard to risk.

risk of exposure: The likelihood of a security incident occurring.

risk treatment: A process to modify risk. Also known as *risk response*.

role-based access control (RBAC): Access control based on user roles (that is, a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions in an organization. A given role may apply to a single individual or to several individuals.

rooting: The process of removing a restricted mode of operation. For example, rooting may enable content with digital rights to be used on any computer, or it may allow enhanced third-party operating systems or applications to be used on a mobile device. While rooting is the term used for Android devices, *jailbreaking* is the equivalent term used for Apple devices.

https://t.me/learningnets

screen lock: A computer–user interface element in various operating systems that regulates immediate access to a device by requiring the user to perform a certain action in order to receive access, such as entering a password, using a certain button combination, or performing a certain gesture using a device's touchscreen.

security awareness: The extent to which staff understand the importance of information security, the level of security required by the organization, and their individual security responsibilities.

security classification: The grouping of information into classes that reflect the value of the information and the level of protection required. Also called *security categorization*.

security controls: The management, operational, and technical controls (that is, countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

security culture: The extent to which staff demonstrate expected security behavior in line with their individual security responsibilities and the level of security required by the organization.

security event: An occurrence considered by an organization to have potential security implications to a system or its environment. Security events identify suspicious or anomalous activity. Events sometimes provide indications that incidents are occurring.

security incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

security objective: The characteristic of security to be achieved, typically consisting of confidentiality, integrity, and availability.

security operations center (SOC): A facility that tracks and integrates multiple security inputs, ascertains risk, determines the targets of an attack, contains the impact of an attack, and recommends and/or executes responses appropriate to a given attack. In some cases, an organization establishes a SOC for itself. In other cases, SOC services are outsourced to a private company that specializes in providing such services.

security performance: The measurable result of security controls applied to information systems and supporting information security programs.

security policy: A set of rules and practices that specify or regulate how a system or an organization provides security services to protect sensitive and critical system resources.

security program: The management, operational, and technical aspects of protecting information and information systems. It encompasses policies, procedures, and management structure and mechanisms for coordinating security activity.

https://t.me/learningnets

self-encrypting drive: A hard drive with a circuit built into the disk drive controller chip that encrypts all data to the magnetic media and decrypts all the data from the media automatically. All self-encrypting drives encrypt all the time from the factory onward, performing like any other hard drive, with the encryption being completely transparent or invisible to the user. To protect the data from theft, the user must provide a password to read from or write data to the disk.

sensitive information: Information that can only be disclosed to authorized individuals (for example, product designs, merger and acquisition plans, medical records, business strategy information).

side-channel attack: An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions.

single sign-on (SSO): A security subsystem that enables a user's identity to be authenticated at an identity provider—that is, at a service that authenticates and asserts the user's identity—and then to have that authentication honored by other service providers.

social engineering: The process of attempting to trick someone into revealing information (for example, a password) that can be used to attack an enterprise or into performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

source code repository: A file archive in which a large amount of source code for software is kept, either publicly or privately. Source code repositories are often used by open source software projects and other multiple-developer projects to handle various versions. They help developers submit code patches in an organized fashion. Often these archives support version control, bug tracking, release management, mailing lists, and wiki-based documentation.

spear phishing: Phishing that is targeted against a group, a company, or individuals within a company.

stakeholder: A person, a group, or an organization that has interest or concern in an organization. Stakeholders can affect or be affected by an organization's actions, objectives, and policies. Some examples of key stakeholders are creditors, directors, employees, government (and its agencies), owners (shareholders), suppliers, unions, and the community from which the business draws its resources.

strategic plan: A document used to communicate with the organization the organization's goals, the actions needed to achieve those goals, and all the other critical elements developed during the planning exercise.

system owner: The person or organization responsible for the development, procurement, integration, modification, operation, maintenance, and final disposition of an information system.

system security plan: A formal document that provides an overview of the security requirements for the information system and describes the security controls that are in place or planned for meeting those requirements.

https://t.me/learningnets

technical security controls: Security controls (that is, safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

technical vulnerability: A hardware, firmware, communication, or software flaw that leaves an information processing system open for potential exploitation either externally or internally, thereby resulting in risk for the system.

threat: A potential for violation of security that exists when there is a circumstance, a capability, an action, or an event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

threat intelligence: The knowledge established as a result of analyzing information about potential or current attacks that threaten an organization. The information is taken from a number of internal and external sources, including application, system, and network logs; security products such as firewalls and intrusion detection systems; and dedicated threat feeds. Also known as *cyber threat intelligence* (*CTI*).

total cost of ownership (TCO): A comprehensive assessment of IT or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses, and the opportunity cost of downtime, training, and other productivity losses.

trust relationship: A relationship between two different domains or areas of authority that makes it possible for users in one domain to be authenticated by a domain controller in the other domain.

user testing: A phase of system development in which the software or system is tested in the "real world" by the intended audience. Also called *end-user testing*.

value proposition: A statement that identifies clear, measurable, and demonstrable benefits consumers get when buying a particular product or service. It should convince consumers that this product or service is better than others on the market.

virtual private network: A restricted-use, logical (that is, artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (that is, real) network (for example, the Internet), often using encryption (located at hosts or gateways) and authentication. The endpoints of the virtual network are said to be tunneled through the larger network.

vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Waterfall development: A method of deploying software or systems in which development moves through a series of fairly well-defined stages. With large projects, once each stage is complete, it cannot be easily reversed, much as it is impossible to move up a waterfall. This traditional system engineering flow allows for a requirements-driven process that leads to assured and verified function. Note that although this indicates a linear sequence through the stages, the ability to iterate and propagate changes discovered in one facet to the others is typically observed.

https://t.me/learningnets

web analytics: The process of analyzing the behavior of visitors to a website. Web analytics involves extracting and categorizing qualitative and quantitative data to identify and analyze onsite and offsite patterns and trends.

whois: An Internet program that allows users to query a database of people and other Internet entities, such as domains, networks, and hosts. The information stored includes a person's company name, address, phone number, and email address.

zero-day threat: The threat of an unknown security vulnerability in a computer software or application for which either a patch has not been released or the application developers are unaware or have not had sufficient time to address the issue. A zero-day attack is also sometimes defined as an attack that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

https://t.me/learningnets

This page intentionally left blank

https://t.me/learningnets

Index

Numbers

***10 Key Facts Businesses Need to Note About the GDPR*, 193**

***2017 Data Breach Investigations Report (Verizon)*, 294**

A

AAL (Authentication Assurance Levels), biometric authentication, 341–347

ABAC (Attribute-Based Access Control), 349, 353–355
- attribute metadata, 355–357
- resources, 357–358

access (system)
- access control, 305, 347
  - ABAC, 349, 353–355
  - ABAC, attribute metadata, 355–357
  - ABAC, resources, 357–358
  - access rights, 348–349
  - ACL, 350–351
  - DAC, 349–351
  - discretionary access control, 312
  - MAC, 349
  - metrics, 358–360
  - objects, 348
  - RBAC, 349, 351–353
  - subjects, 348
- authorization, 305, 306–307
- best practices, 362–363
- customer access
  - arrangements, 360
  - connections, 361
  - contracts, 361
  - data security, 361
  - defined, 360
- functions of, 305
- user authentication, 304, 307
  - authenticators, 311
  - biometric authentication, 330–331
  - biometric authentication, AAL, 341–347
  - biometric authentication, accuracy of, 333, 335–336
  - biometric authentication, artifact detection, 340
  - biometric authentication, biometric spoofing, 339
  - biometric authentication, costs of, 333
  - biometric authentication, criteria for, 331
  - biometric authentication, cryptographic devices, 345
  - biometric authentication, FMR, 335–336
  - biometric authentication, FNMR, 335–336
  - biometric authentication, liveness detection, 340
  - biometric authentication, lookup secrets, 345
  - biometric authentication, memorized secrets, 345
  - biometric authentication, operating characteristic curves, 336
  - biometric authentication, operation of, 333–335

https://t.me/learningnets

biometric authentication, OTP devices, 345
biometric authentication, PAD, 339–340
biometric authentication, physical characteristics used in, 332–333
biometric authentication, presentation attacks, 339–340
biometric authentication, risk assessment, 341–347
biometric authentication, security controls, 339–341
biometric authentication, threats to, 337–339
factors of, 310–311
hardware tokens, 322
hardware tokens, eID cards, 325–327
hardware tokens, memory cards, 322–323
hardware tokens, OTP devices, 328–329
hardware tokens, security controls, 330
hardware tokens, smart cards, 323–325
hardware tokens, threats to, 329–330
inherence factor, 310
knowledge factor, 310
multifactor authentication, 311–312
passwords, 312
passwords, blacklists, 321
passwords, cracking, 317–319
passwords, file access control, 319–320
passwords, hashed passwords, 315–316
passwords, OTP devices, 328–329
passwords, PACE, 327
passwords, regulating password selection, 321
passwords, shadow password files, 319
passwords, system-selected passwords, 321–322
passwords, UNIX password schemes, 315–316
passwords, user-selected passwords, 320
passwords, vulnerabilities, 313–315
possession factor, 310

accessibility
increased accessibility, privacy threats, 191
remote access security, ICS, 230

accidental behavior (culture of security), 169
account attacks (specific), 313
accountability, 5
accounting management, 393, 395–396
accreditation
C&A, 266, 270
Security Accreditation Packages, 269
security accreditation. *See* authorization
ACL (Access Control Lists), 350–351
acquisition phase (HAM), 214
active monitoring, 511–512
actuators, ICS, 224
address books, office equipment threats/vulnerabilities, 218
administration, port administration, VoIP networks, 443
adware, 91, 487
aggregation, privacy threats, 190
AI (Artificial Intelligence), non-malware attacks, 577
algorithms (cryptographic), 518
ALM (Application Life Cycle Management), 257–259, 281–283
AM (Application Management), 280–281
ALM, 281–283
APFM, 283
defined, 283
matrix, dimensions of, 283–284
portfolio management practices, 284–285
reengineering, 284
APM, 285–286
defined, 286
steps of, 286–287
application security, 287
business application registers, 287–288
external application security, 289
internal application security, 288–289
web applications, 293
web applications, policies, 294–295
web applications, risks, 289–291
web applications, WAF, 291–293
best practices, 300–301

https://t.me/learningnets

defined, 281
EUDA, 295–296, 301
benefits of, 296
risks of, 296–297
security framework, 297–300
TCO, 281–283
anomaly detection (intrusion detection), 504–505
antivirus software
cyber attack kill chains, 574
real-time antivirus software, VoIP networks, 443
AP (Access Points)
NAP, physical network management, 423
rogue AP, wireless network security, 427
WAP
network management, 416
SSID, 426
APFM (Application Portfolio Management), 283
defined, 283
matrix, dimensions of, 283–284
portfolio management practices, 284–285
reengineering, 284
APM (Application Performance Management), 285–286
defined, 286
steps of, 286–287
app stores, 236
application whitelisting
defined, 164
ICS, 229
application-layer firewalls, VoIP networks, 443
application-level gateways (stateful inspection firewalls), 413
applications
backups, 641–642
cloud-based applications, security, 232
EUDA, 295–296, 301
benefits of, 296
risks of, 296–297
security framework, 297–300
security, 287
business application registers, 287–288
external application security, 289
internal application security, 288–289
web applications, 293
web applications, policies, 294–295
web applications, risks, 289–291
web applications, WAF, 291–293
technology stacks, 234
unknown authorship of, 237
vetting process, 240–241
web applications
Open Web Application Security Project, 290–291
security, 293
security, policies, 294–295
security, risks, 289–291
security, WAF, 291–293
appropriation, privacy threats, 191
APT (Advanced Persistent Threats), 566
architectures
defined, 58
enterprise architectures, 59
FEAF, 58–59
RM, 59–62
security governance integration, 58
information security architectures, 58
ARM (Application Reference Models), 60–61
arrangements (customer), access control, 360
artifact detection, biometric authentication, 340
assets
asset register, 87–88
business assets, defined, 87
defined, 4, 75–77
hardware assets, defined, 85
identifying, 84–85
information assets, defined, 86–87
physical asset management, 210–211
CMDB, 212
HAM, 211–212

https://t.me/learningnets

HAM, acquisition phase, 214
HAM, average life cycle duration of common hardware, 216
HAM, deployment phase, 214–215
HAM, disposition phase, 216
HAM, management phase, 215–216
HAM, planning phase, 213–214
ICS, defined, 223
ICS, elements of, 224–225
ICS, IT systems versus, 225–228
ICS, security, 227–228, 229–231
ICS, threats/vulnerabilities, 228–229
mobile devices, ecosystem of, 234–236
mobile devices, security, 231–233
mobile devices, technology stacks, 233–234
office equipment, 217
office equipment, cryptographic erasure, 222–223
office equipment, disposal of, 222–223
office equipment, OS security, 219
office equipment, physical security, 219
office equipment, security controls, 219–222
office equipment, threats/vulnerabilities, 217–219
risk assessment, determining future problems, 79
RM assets, 62
software assets, defined, 85

ATE (Awareness, Training, Education), 172

attack surfaces
defined, 230
reducing, ICS, 230

attacks
brute-force attacks, 532
cyber attacks, defined, 570
DDoS attacks
cyber attack kill chains, 575
defined, 575
DoS attacks, servers, 368
exploits, defined, 566
man-in-the-middle attacks, VoIP, 443
non-malware attacks, 576–577
offline dictionary attacks, 313
password guessing, 313
phishing, defined, 565
popular password attacks, 313
presentation attacks, 339–340
side-channel attacks, 242
social engineering attacks, defined, 571
source routing attacks, 411
spear phishing, defined, 571
specific account attacks, 313
tiny fragment attacks, 411

audits
business continuity readiness, 653–654
ERM committees, 66
security audits
controls, 673–677
data collection, 668–672
defined, 666–667
elements of, 668
external audits, 672–673
internal audits, 672
logs, 671–672
objectives of, 667
security audit trails, 667, 671–672

AUP (Acceptable Use Policies), 146, 152–153
email, 434–435
IM, 436–437
SANS Institute AUP template, 152–153

authentication
DANE, 433
device authentication, VoIP networks, 443
digital authentication, 308
DMARC, 433
managing, ICS, 230
MFA, 230
possession-based authentication. *See* hardware tokens
user authentication, 304, 307
authenticators, 311
biometric authentication, 330–331
biometric authentication, AAL, 341–347
biometric authentication, accuracy of, 333, 335–336

https://t.me/learningnets

biometric authentication, artifact detection, 340
biometric authentication, biometric spoofing, 339
biometric authentication, costs of, 333
biometric authentication, criteria for, 331
biometric authentication, cryptographic devices, 345
biometric authentication, FMR, 335–336
biometric authentication, FNMR, 335–336
biometric authentication, liveness detection, 340
biometric authentication, lookup secrets, 345
biometric authentication, memorized secrets, 345
biometric authentication, operating characteristic curves, 336
biometric authentication, operation of, 333–335
biometric authentication, OTP devices, 345
biometric authentication, PAD, 339–340
biometric authentication, physical characteristics used in, 332–333
biometric authentication, presentation attacks, 339–340
biometric authentication, risk assessment, 341–347
biometric authentication, security controls, 339–341
biometric authentication, SP 800-63B guidelines, 340–341
biometric authentication, threats to, 337–339
cryptography and, 518
factors of, 310–311
hardware tokens, 322
hardware tokens, eID cards, 325–327
hardware tokens, memory cards, 322–323
hardware tokens, OTP devices, 328–329
hardware tokens, security controls, 330
hardware tokens, smart cards, 323–325
hardware tokens, threats to, 329–330
inherence factor, 310
knowledge factor, 310
multifactor authentication, 311–312
NIST SP 800-63 Digital Identity Model, 307–310
passwords, 312
passwords, blacklists, 321
passwords, cracking, 317–319
passwords, file access control, 319–320
passwords, hashed passwords, 315–316
passwords, OTP devices, 328–329
passwords, PACE, 327
passwords, regulating password selection, 321
passwords, shadow password files, 319
passwords, system-selected passwords, 321–322
passwords, UNIX password schemes, 315–316
passwords, user-selected passwords, 320
passwords, vulnerabilities, 313–315
possession factor, 310
VoIP networks, 443

authenticity, 5

authorization, 305, 306–307

operations/maintenance phase (NIST SDLC), 272
security, 269, 270

automation, passwords, 314

auto-rooters, 91, 488

availability, 5

avoidance controls, 100

B

backdoors (trapdoors), 91, 488

background checks/screening, 162–163

backups

application backups, 641–642
cold site backups, 385
data restoration from backups, cyber attack kill chains, 574
hot site backups, 386
systems management, 384–386
warm site backups, 386

BCM (Business Continuity Management), 623, 625

https://t.me/learningnets

application backups, 641–642
BCMS, 625
BCP, 625, 642
components of, 642–644
crisis management plans, 645–646
emergency response plans, 644–645
governance, 630–631
overview of, 643–644
recovery/restoration plans, 646–647
best practices, 660
BIA, 631–632
business continuity readiness
awareness, 637–638
BCP, 642–647
control selection, 640–642
exercising/testing, 647–650
performance evaluations, 650–654
resilience, 639–640
training, 638–639
business continuity strategies
cost balancing, 634–635
determination/selection, 635–636
protection/mitigation, 637
resource requirements, 636–637
business resilience, 639–640
components of, 630
COOP, defined, 630
crisis management plans, 656–657
effectiveness of, 628–629
elements of, 623
emergency response plans, 655–656
ICT supply chains, 630
incident response process, 659
objectives of, 629
process of, 655
recovery/restoration plans, 657–659
resources, 622–623
risk assessment, 632–634
threats
cyber attacks, 627
human-caused physical threats, 627–628
natural disasters, 626
system problems, 627

BCMS (Business Continuity Management Systems), 625

BCP (Business Continuity Plan), 625, 642
components of, 642–644
crisis management plans, 645–646
emergency response plans, 644–645
governance, 630–631
overview of, 643–644
recovery/restoration plans, 646–647

behaviors (culture of security)
accidental behavior, 169
malicious behavior, 168–169
negligent behavior, 168

best practices
AM, 300–301
BCM, 660
cloud computing, 476–477
communications, 444–445
cryptography, 542
DRM, 515–517, 542
IAM, 501–502, 542
IDS, 508–509
incident management, 597–598
information management, 205–206
intrusion detection, 508–509, 542
local environment security, 619
malware, 541
network management, 444–445
people management, 175–176
physical asset management, 244–245
physical security, 619
PKI, 542
risk assessment, 131–132
SCM, 478–479
SCRM, 463–466
security governance, 69–70
security incident management frameworks, 597–598
security management, 154
security monitoring, 691–692
SEM, 561–563
system access, 362–363
system development, 278

https://t.me/learningnets

systems management, 389–390
technical security management, 541–542
best practices and standards documents, 6–7, 36–37
CIS CSC, 27–28
COBIT 5 for information security, 29–30
ISO/IEC 27000 suite of information security standards, 12–13
ISMS, 13–15
ISO 27001, 14, 15–16
ISO 27002, 14, 17–18
ISO 27005, 15
ISO 27014, 15
ISO 27036, 15
mapping to ISF SGP, 18–21
ITU-T security documents, 32–34
NIST cybersecurity framework and security documents, 21–22, 25–26
components of, 22–25
FIPS 200, 26
FIPS 800-27, 26
SP 800-12, 26
SP 800-55, 26
SP 800-100, 26
SP 800-144, 26
SP 1800, 26
PCI-DSS, 30–32
Standard of Good Practice for Information Security (SGP), 7–10
areas of, 10–12
categories of, 10–12
mapping ISO 27000 suite to ISF SGP, 18–21
BIA (Business Impact Analysis), 631–632
biometric authentication, 330–331
AAL, 341–347
accuracy of, 333, 335–336
artifact detection, 340
biometric spoofing, 339
costs of, 333
criteria for, 331
cryptographic devices, 345
FMR, 335–336
FNMR, 335–336
liveness detection, 340
lookup secrets, 345
memorized secrets, 345
operating characteristic curves, 336
operation of, 333–335
OTP devices, 345
PAD, 339–340
physical characteristics used in, 332–333
presentation attacks, 339–340
risk assessment, 341–347
security controls, 339–341
SP 800-63B guidelines, 340–341
threats to, 337–339
biometric spoofing, 339
BIRT (Business Impact Reference Tables), 126–127
blacklists, 321
blackmail, privacy threats, 191
blockchains, 95
bots (zombies), 91, 489
breach of confidentiality, privacy threats, 190
BRM (Business Reference Models), 60
brute-force attacks, 532
business application management. *See* AM (Application Management)
business application registers, 287–288
business assets, 87
Business Continuity Management (BCM), 623, 625
application backups, 641–642
BCMS, 625
BCP, 625, 642
components of, 642–644
crisis management plans, 645–646
emergency response plans, 644–645
governance, 630–631
overview of, 643–644
recovery/restoration plans, 646–647
best practices, 660
BIA, 631–632
business continuity readiness
awareness, 637–638
BCP, 642–647
control selection, 640–642

https://t.me/learningnets

exercising/testing, 647–650
performance evaluations, 650–654
resilience, 639–640
training, 638–639
business continuity strategies
cost balancing, 634–635
determination/selection, 635–636
protection/mitigation, 637
resource requirements, 636–637
business resilience, 639–640
components of, 630
COOP, defined, 630
crisis management plans, 656–657
effectiveness of, 628–629
elements of, 623
emergency response plans, 655–656
ICT supply chains, 630
incident response process, 659
objectives of, 629
process of, 655
recovery/restoration plans, 657–659
resources, 622–623
risk assessment, 632–634
threats
cyber attacks, 627
human-caused physical threats, 627–628
natural disasters, 626
system problems, 627
business resource threats, 89
BYOD (Bring Your Own Device) policies, 173

C

C&A (Certification and Accreditation), 266, 270
C-level roles/responsibilities, 55
CA (Certification Authorities), 539–540
cables, telecommunication cables, physical network management, 423
capacity management, 383–384
capacity planning, 138
capital planning, security planning
information security costs, 144–145
investment lifecycle, 142–145
CCB (Change Control Boards)
defined, 271
NIST SDLC security
disposal phase, 273
operations/maintenance phase, 272
CEO (Chief Executive Officers)
ERM committees, 65
security governance, 55
CERT (Computer Emergency Response Teams), vulnerability management, 548–549
certificates (public key), 536–538
certifications
C&A, 266, 270
CISM, 175
CISSP, 175
defined, 15
GSEC, 174
SANS computer security training and certification, 175
security awareness/education, 174–175
SSCP, 175
CFO (Chief Financial Officers), ERM committees, 65
change control
CCB
defined, 271
NIST SDLC security, disposal phase, 273
NIST SDLC security, operations/maintenance phase, 272
defined, 271
change management, 169, 386–389
characteristic curves, biometric authentication, 336
Chase Bank online privacy policy, 190
CIO (Chief Information Officers), security governance, 55
circuit-level gateways (stateful inspection firewalls), 413–414
CIS (Center of Internet Security), CIS CSC, 27–28
Cisco Annual Cybersecurity Reports, 98

https://t.me/learningnets

CISM (Certified Information Security Manager), 175
CISO (Chief Information Security Officers)
COBIT 5, 64
ERM committees, 65
ISS committees, 65
security governance, 55
security management, 137
security management, role in, 138–140
CISSP, 175
classifying
information, 179
labeling information, 185
NIST risk management framework, 179–183
RFID tags, 185
security classification process, 183–185
threats, 89–90
clickless malware, 490
cloud computing
applications, security, 232
best practices, 476–477
cloud auditors, 471, 472
cloud brokers, 471–472
cloud carriers, 471, 472
cloud consumers, 471–472
cloud service providers, 382–383
community clouds, 468
context of, 468–469
CP, 471–472
defined, 466
deployment models, 468–470
elements of, 466–467
hybrid clouds, 468
IaaS, 468, 472
PaaS, 468, 472
private clouds, 468–469
public clouds, 468, 469–470
reference architecture, 470–472
risk assessment, 475–476
SaaS, 467–468
security, 473
risk assessment, 475–476
threats, 474–475
service agreements, 477–478
service models, 467–468
threats, 474–475
CMDB (Configuration Management Database), 212
COBIT 5 (Control Objectives for Business and Related Technology 5)
change management, 386
information security, 29–30
CISO, 64
ERM committees, 65
information custodians, 65
ISM, 65
ISS committees, 64
RACI charts, 66–67
security governance, 64–66
sensitive information management, 204–205
code injection, 92
coding, mobile codes, 91
cold site backups, 385
collecting information, threats to privacy, 189
communications, 430
best practices, 444–445
email, 430–431
AUP, 434–435
DANE, 433
DKIM, 433
DMARC, 433
MDA, 432
MS, 432
MSA, 432
MTA, 432
MUA, 431–432
S/MIME, 433
SPF, 433
STARTTLS, 433
trustworthy email standards, 432–434
IM, 436
AUP, 436–437
security policies, 437–438
IP telephony/conferencing, 444

https://t.me/learningnets

VoIP networks, 438
context, 440–442
processing, 439–440
security, 443
signaling, 439
threats, 442–443
community clouds, 468
compliance monitoring, security performance, 690–691
conferencing/IP telephony, 444
confidentiality, 5, 190
configuration management, 393, 396–397
defined, 139
ICS, 230
security management and, 139
connection reviews. *See* ORR
connections (customer), access control, 361
container virtualization, 85, 374
contingency planning and security management, 139
contingency training, 267–269
contracts (customer), access control, 361
control gates, NIST SDLC security, 260
development/acquisition phase, 266
implementation/assessment phase, 270
initiation phase, 263
operations/maintenance phase, 272
controllers, ICS, 225
controls
avoidance controls, 100
checklist of controls, 101–102
deterrent controls, 100–101
identifying, 98–99
online catalog of security controls, 99–100
responsive controls, 101
vulnerability controls, 101
COO (Chief Operating Officers)
ERM committees, 65
security governance, 55
COOP (Continuity of Operations), 630
COPPA (Children's Online Privacy Protection Act), 195
copy/scan logs, office equipment threats/vulnerabilities, 218
costs
balancing, business continuity strategies, 634–635
cybersecurity, 6
risk assessment, 108
COTS (Commercial-Off-The-Shelf) software, 288
countermeasures, 26
CP (Cloud Providers), 471–472
CPO (Chief Privacy Officers), security governance, 55
crackers (hackers), 92
cracking passwords, 317–319
credentials
CSP, 308
defined, 309
crisis management plans, 645–646, 656–657
critical information, 171
Critical Security Controls for Effective Cyber Defense (CSC), 27–28
CRO (Chief Risk Officers)
ERM committees, 66
security governance, 55
cryptanalysis, 532
cryptographic devices, biometric authentication, 345
cryptographic erasure, 222–223
cryptography
algorithms, 518, 525
best practices, 542
data encryption, 517–518
data integrity, 518
digital signatures, 518, 524–525
implementation considerations, 526–528
key management
cryptoperiods, 532–533
cryptosystems, 528
group keys, 530
key life cycles, 534–536
resources, 529–530
types of keys, 530–531

https://t.me/learningnets

public key encryption, 520–521
secure hash functions, 522–524
symmetric encryption, 518–520
user authentication, 518
uses of, 517–518
cryptoperiods, 532–533
CSC (Critical Security Controls for Effective Cyber Defense), 27–28
CSIRT (Computer Security Incident Response Teams), 381–382
CSO (Chief Security Officers), security governance, 55
CSP (Credential Service Providers), 308
CTI (Cyber Threat Intelligence). *See* threat intelligence
culture of security, 168
customer access
arrangements, 360
connections, 361
contracts, 361
data security, 361
defined, 360
CVSS metrics, NVD, 105–107
cyber attack kill chains, 570
actions phase, 573, 575
command-and-control phase, 573, 575
delivery phase, 572, 573–574
exploit phase, 572, 574
installation phase, 572, 574–575
non-malware attacks, 576–577
reconnaissance phase, 570–571, 573
weaponization phase, 571, 573
cyber attacks
BCM, 627
defined, 570
cybersecurity
accountability, 5
authenticity, 5
availability, 5
benefits of, 6
confidentiality, 5
costs of, 6
defined, 3
essentials program, 173
information security, 4, 68–69
COBIT 5, 29–30, 64–66
information security architectures, 58
information security governance, defined, 42–43
information security reports, 53–55
information security standards, 12–21
information security strategic planning, 50
Standard of Good Practice for Information Security (SGP), 9–12
integrity, 5
learning continuum, phases of, 167
management process, 34–37
network security, 4
nonrepudiation, 5
objectives of, 4–5
user needs versus security implementation, 6
cyberspace
complexity of, 5
defined, 3
scale of, 5

D

DAC (Discretionary Access Control), 349–351
DANE (DNS-based Authentication of Named Entities), 433
DAS (Direct Access Storage), 377
data at rest (DLP), 510–511
data breaches, 294
data encryption, 517–518
data in motion (or transit), DLP, 510, 511–512
data in use (DLP), 510, 512
data integrity, 518
data restoration from backups, cyber attack kill chains, 574
data tampering, 89
databases, fingerprinting, 509
DBIR (Data Breach Investigations Reports), 93–94
DDoS (Distributed Denial-of-Service) attacks
cyber attack kill chains, 575
defined, 92, 575

https://t.me/learningnets

de-perimeterization, mobile devices, 232
decisional interference, privacy threats, 191
defense in depth strategies (physical security), 610–612
deployment phase (HAM), 214–215
deployment reviews. *See* ORR
deterrent controls, 100–101
development/acquisition phase (NIST SDLC), 250–251, 264–266
device authentication, VoIP networks, 443
DevOps, 254–256
ALM, 257–259
defined, 254
reference architecture, 255–257
diagnostics (remote), ICS, 225
dictionary attacks (offline), 313
digital authentication, 308
digital signatures, 518, 524–525
directory servers, 164
disclosure, privacy threats, 190
disclosure of information, office equipment threats/vulnerabilities, 218
discretionary access control, 312
disposal phase (NIST SDLC), 252, 272–273
disposing of office equipment, 222–223
disposition phase (HAM), 216
disseminating information, threats to privacy, 190–191
distortion, privacy threats, 191
distributed network management systems, 401–402
DKIM (DomainKeys Identified Mail), 433
DLP (Data Loss Prevention), 186, 509
classifying data, 509–510
data at rest, 510–511
data in motion (or transit), 510, 511–512
data in use, 510, 512
database fingerprinting, 509
exact file matching/hash values, 510
partial document matching, 510
rule-based recognition, 509
DMARC (Domain-based Message Authentication, Reporting and Conformance), 433
DMZ (Demilitarized Zones), 508
DMZ networks and firewalls, 414–416
DNS attacks, 92
documents, 140–141
AUP, 146, 152–153
awareness program communication materials, 170–172
BCP, 642
components of, 642–644
crisis management plans, 645–646
emergency response plans, 644–645
overview of, 643–644
recovery/restoration plans, 646–647
best practices and standards documents, 6–7, 8–12
change request documents, 388
crisis management plans, 645–646
emergency response plans, 644–645
employment agreements, 163
information security reports, 53–55
information security strategic planning, 146
managing, 198–202
network documentation, physical network management, 423
partial document matching, 510
RACI charts, security governance, 66–67
recovery/restoration plans, 646–647
risk assessment reports, 92–93
Cisco Annual Cybersecurity Reports, 98
ENISA Threat Landscape Reports, 95–96
Fortinet Threat Landscape Reports, 98
Threat Horizon Reports, 94–95
Trustwave Global Security Reports, 97
Verizon DBIR, 93–94
Router and Switch Security Policy (SANS Institute), 148–150
security planning, 146
AUP, 146, 152–153
information security strategic planning, 146
Router and Switch Security Policy (SANS Institute), 148–150
security policies, 146
security policies, templates, 147–150

https://t.me/learningnets

simple risk analysis worksheet, 113–114
templates
Router and Switch Security Policy (SANS Institute), 148–150
security planning, 147–150
security policy templates, 147–150
DoS (Denial-of-Service) attacks, 90
defined, 92
office equipment, 218–219
servers, 368
downloaders, 91, 488
DRM (Data Reference Models), 60
DRM (Data Rights Management), 512
architecture of, 514–515
best practices, 515–517, 542
components of, 513–514
droppers, 91, 488
dual operator policies, human resource security, 165
duties, separation of, human resource security, 165

E

eavesdropping
VoIP, 443
wireless network security, 427
eID (Electronic Identification) cards, 325–327
Electronic Communications Privacy Act, The, 195
element management layer (network management systems), 403
elevation of privileges, 90
email, 430–431
AUP, 434–435
DANE, 433
DKIM, 433
DMARC, 433
MDA, 432
MS, 432
MSA, 432
MTA, 432
MUA, 431–432
S/MIME, 433
SPF, 433
STARTTLS, 433
trustworthy email standards, 432–434
emergencies (security incident), handling, 590–592
emergency response plans, 644–645, 655–656
EMI (Electromagnetic Interference), 609
EMM systems, mobile devices, 242–243
employees, security
awareness/education, 166, 168
awareness program communication materials, 170–172
awareness program evaluation, 172
certification, 174–175
culture of security, 168
cybersecurity essentials program, 173
cybersecurity learning continuum, phases of, 167
NIST ATE, 172
processes of, 169–170
role-based training, 173–174
SP 800-16, 166
SP 800-50, 166
current employees, 164–165
dual operator policies, 165
limited reliance on key employees, 165
privileges, 165
remote working, 176
separation of duties, 165
termination of employment, 165–166
vacations, 165
employment agreements, 163
encryption
cryptographic erasure, 222–223
data encryption, 517–518
public key encryption, 520–521
symmetric encryption, 518–520
VoIP networks, 443
end-user testing, 265
ENISA Threat Landscape Reports, 95–96, 294
enterprise architectures, 59
FEAF, 58–59
RM, 59–60

https://t.me/learningnets

ARM, 60–61
assets of, 62
BRM, 60
DRM, 60
IRM, 61
PRM, 60
relationships between components, 61
SRM, 61–62
security governance integration, 58
enterprise infrastructures, mobile devices, 242–243
enterprise strategic planning, 47
environment security, 275–277
environmental threats
BCM, 626
defined, 89
local environment security, 607–608, 612–614
equipment disposal, 222–223
erasing data, cryptographic erasure, 222–223
ERM (Enterprise Risk Management) committees
COBIT 5, 65
ERM committees, 65–66
EUDA (End-User-Developed Applications), 295–296, 301
benefits of, 296
risks of, 296–297
security framework, 297–300
evaluating, risk, 76
events
defined, 75
threat event frequency, estimating, 118–119
exact file matching/hash values, 510
exclusion, privacy threats, 190
exfiltration, 457
exploit kits, 91
exploits, 488
defined, 91, 566
website exploits, defined, 92
exposure
privacy threats, 190
RoE, 76
external network connections, managing, 427–428
external requirements function, security management, 140

F

FACTA (Fair and Accurate Credit Transaction Act of 2003), 195
FAIR (Factor Analysis of Information Risk), 114
impact assessment, 122–123
BIRT, 126–127
loss estimation, 123–126
likelihood assessments, 116–118
loss estimation, 123–126
loss event frequency, 121–122
Open Group security standards, 114–115
risk assessment, 115–116
risk assessment matrices, 120–121
false negatives (intrusion detection), 504–505
false positives (intrusion detection), 504–505
fault management, 393, 394–395
fax logs, office equipment threats/vulnerabilities, 218
FEAF (Federal Enterprise Architecture Framework), 58–59
Federal Policy for the Protection of Human Subjects, 195
federated identity management, 498–500
FERPA (Family Educational Rights and Privacy Act of 1974), 195
file access control and passwords, 319–320
fileless malware, 490
fingerprinting (database), 509
firewalls, 404
application-layer firewalls, VoIP networks, 443
characteristics of, 404–405
cyber attack kill chains, 574, 575
DMZ networks, 414–416
limitations of, 406
network-based firewalls, 292
next-generation firewalls, 414

https://t.me/learningnets

packet filtering firewalls, 406–411
planning, 428–429
policies, 428
stateful inspection firewalls, 411–413
application-level gateways, 413
circuit-level gateways, 413–414
VPN (firewall-based), 420
WAF, 291–293, 574
firmware, technology stacks, 234
flooders, 91, 488
flows (ICT supply chains), 450–451
FMR (False Match Rates), biometric authentication, 335–336
FNMR (False Nonmatch Rates), biometric authentication, 335–336
forensics, 592–593
analysis phase, 595–596
collection phase, 594–595
identification phase, 594
incident management, 584
preparation phase, 593–594
preservation phase, 595
reporting phase, 596
Fortinet Threat Landscape Reports, 98
functional testing, 265

G

gateways, stateful inspection firewalls
application-level gateways, 413
circuit-level gateways, 413–414
GDPR (General Data Protection Regulation), 193–195
GIAC (Global Information Assurance Certification), GSEC, 174
GLBA (Gramm-Leach-Bliley Act of 1999), 195
golden records, ICS, 231
Google privacy policy, 190
governance (security)
BCP, 630–631
best practices, 69–70
CEO, 55
CIO, 55
CISO, 55
components of, 47
COO, 55
CPO, 55
CRO, 55
CSO, 55
defined, 43
desired outcomes, 46
effectiveness of, 68–69
enterprise architecture integration, 58
evaluating, 68–69
framework of, 63
information security architectures, 58
governance, defined, 42–43
ISMS, 44
principles of, 45–46
reporting relationships for, 56
roles/responsibilities of, 55, 57–58
security direction
COBIT 5, 64–66
ISF SGP, 64
RACI charts, 66–67
security management and, 138
security programs, defined, 43
stakeholders, defined, 45–46
strategic planning, 47
defined, 48
enterprise strategic planning, 47
framework of, 51–52
information security strategic planning, 50
IT strategic planning, 48–49
GPS (location services), security, 237
group key cryptography, 530
GSEC (Global Security Essentials), 174
guessing passwords, 313
guest OS (VM), 371

H

hackers (crackers)
defined, 92
wireless network security, 427

https://t.me/learningnets

HAM (Hardware Asset Management), 211–212
acquisition phase, 214
average life cycle duration of common hardware, 216
deployment phase, 214–215
disposition phase, 216
management phase, 215–216
planning phase, 213–214
hard drives, SED, 222
hardware assets
CMDB, 212
defined, 85
HAM, 211–212
acquisition phase, 214
average life cycle duration of common hardware, 216
deployment phase, 214–215
disposition phase, 216
management phase, 215–216
planning phase, 213–214
hardware, technology stacks, 233–234
hardware tokens, 322
eID cards, 325–327
memory cards, 322–323
OTP devices, 328–329
security controls, 330
smart cards, 323–325
threats to, 329–330
hash functions (secure), 522–524
hash values/exact file matching, 510
hashed passwords, 315–316
HIDS (Host-based Intrusion Detection Systems), 503, 505–506, 574
hijacking workstations, 313
HIPAA (Health Insurance Portability and Accountability Act of 1996), 195
hiring process, security, 162
background checks/screening, 162–163
directory servers, 164
employment agreements, 163
job descriptions, 164
hosted (nested) virtualization, 372
hosted virtualization security, 377
hostile actors, threat identification, 89
hot site backups, 386
human resource security, 160–162
current employees, 164–165
dual operator policies, 165
hiring process, 162
background checks/screening, 162–163
directory servers, 164
employment agreements, 163
job descriptions, 164
limited reliance on key employees, 165
privileges, 165
remote working, 176
separation of duties, 165
termination of employment, 165–166
vacations, 165
human-caused physical threats
BCM, 627–628
local environment security, 609, 615
human-machine interface, ICS, 225
hybrid clouds, 468
hypervisors, 371
functions of, 371
security, 376
types of, 371–374

I

IaaS (Infrastructure as a Service), 468, 472
IAM (Identity and Access Management), 496
architecture of, 497–498
best practices, 501–502, 542
defined, 496
federated identity management, 498–500
planning, 500–501
SSO, 497
ICS (Industrial Control Systems)
actuators, 224
application whitelisting, 229
attack surfaces, reducing, 230
authentication management, 230

https://t.me/learningnets

configuration management, 230
controllers, 225
defined, 223
elements of, 224–225
golden records, 231
human-machine interface, 225
IT systems versus, 225–228
maintenance, 225
monitoring security, 231
patch management, 230
remote access security, 230
remote diagnostics, 225
security, 227–228, 229–231
sensors, 224
threats/vulnerabilities, 228–229
ICT supply chains
BCM, 630
defined, 449
flows, 450–451
SCRM, 453–456
security controls, 460–463
threats, 456–459
vulnerabilities, 459–460
identification, 307–310, 321
eID cards, 325–327
privacy threats, 190
identifying risk, 76
identity
federated identity management, 498–500
IAM, 496
architecture of, 497–498
best practices, 501–502, 542
defined, 496
federated identity management, 498–500
planning, 500–501
SSO, 497
proofing, 308
spoofing, 89
IDS (Intrusion Detection Systems), 502–503
best practices, 508–509
HIDS, cyber attack kill chains, 574
NIDS, cyber attack kill chains, 575
IEC (International Electrotechnical Commission), ISO/IEC 27000 suite of information security standards, 12–13
ISMS, 13–15
ISO 27001, 14, 15–16
ISO 27002, 14, 17–18
ISO 27005, 15
ISO 27014, 15
ISO 27036, 15
mapping to ISF SGP, 18–21
IM (Instant Messaging), 436
AUP, 436–437
security policies, 437–438
impact (risk management)
defined, 75
determining risk, 77
impact assessment, 122–123
BIRT, 126–127
loss estimation, 123–126
implementation/assessment phase (NIST SDLC), 251–252, 266–270
incident handling checklist, 589
incident management, 577–578
best practices, 597–598
emergencies, handling, 590–592
forensics, 592–593
collection phase, 594–595
identification phase, 594
preparation phase, 593–594, 595–596
preservation phase, 595
reporting phase, 596
gathering information, 583
incident handling checklist, 589
incident response process, 584–585
containment/eradication/recovery phase, 587–588
detection/analysis phase, 586–587
incident handling checklist, 589
post-incident activity phase, 588–589
preparation phase, 585
ISMS and, 579–580
objectives of, 579

https://t.me/learningnets

policies, 580–581
resources, 578–579
roles/responsibilities of, 581–582
tools, 583–584
incident response
BCM, 659
security management and, 139
increased accessibility, privacy threats, 191
information
assets, defined, 86–87
collecting, threats to privacy, 189
disclosure, 90, 218
disseminating, threats to privacy, 190–191
flows (supply chains), 450–451
invasions, threats to privacy, 190–191
labeling, 185
leakage. *See* DLP (Data Loss Prevention)
processing, threats to privacy, 189–190
information custodians
COBIT 5, 65
ERM committees, 66
ISS committees, 65
information management, 178–179
best practices, 205–206
classifying information, 179
labeling information, 185
NIST risk management framework, 179–183
RFID tags, 185
security classification process, 183–185
document/records management, 198–199
differences between documents and records management, 199–200
document management, 200–202
records management, 202–204
handling information, 186
privacy, 186–188
Chase Bank online privacy policy, 190
collecting information, 189
disseminating information, 190–191
Google privacy policy, 190
invasions, 190–191
principles/policies, 191–198
privacy controls, 196–198
processing information, 189–190
security's relationship to privacy, 188
threats to privacy, 189–191
U.S. privacy laws/regulations, 195
sensitive information, 204–205
information protection champions, 605–606
information security, 4, 68–69
architectures, 58
COBIT 5
CISO, 64
COBIT 5 for information security, 29–30
coordinators, 604–605
governance, defined, 42–43
ISMS, 44
ISO/IEC 27000 suite of information security standards, 12–13
ISMS, 13–15
ISO 27001, 14, 15–16
ISO 27002, 14, 17–18
ISO 27005, 15
ISO 27014, 15
ISO 27036, 15
mapping to ISF SGP, 18–21
management, defined, 43
reports, 53–55
Standard of Good Practice for Information Security (SGP), 9–12, 18–21
strategic planning, 50, 146
information system resilience, 639
inherence factor (user authentication), 310
initiation phase (NIST SDLC), 249–250, 260–263
injection flaws, 92
insecurity, privacy threats, 190
integration testing, 251
integrity, 5, 518
interrogation, privacy threats, 189
intrusion, privacy threats, 191
intrusion detection, 502, 504
anomaly detection, 504–505
best practices, 508–509, 542

https://t.me/learningnets

false negatives, 504–505
false positives, 504–505
HIDS, 503, 505–506
IDS, 502–503, 508–509
misuse detection, 504
NIDS, 503, 506
deploying, 507–508
function of, 506
principles of, 503–504
true negatives, 505
true positives, 505

invasions of privacy, information management, 190–191

investment lifecycles, capital planning, security planning, 142–145

IP address spoofing, 411

IP telephony/conferencing, 443–444

IPR (Intellectual Property Rights), 455

IPS (Intrusion Protection Systems), cyber attack kill chains, 574

IPSec (IP Security), 418–420

IRM (Infrastructure Reference Models), 61

ISACA, CISM, 175

ISC (Internet Storm Center)
CISSP, 175
SSCP, 175
vulnerability management, 549

ISF (Information Security Forum)
SGP, security governance, 64
Standard of Good Practice for Information Security (SGP), 7–10
areas of, 10–12
categories of, 10–12
mapping ISO 27000 suite to ISF SGP, 18–21
Threat Horizon Reports, 94–95

ISM (Information Security Managers)
COBIT 5 for information security, 65
ISS committees, 65
security management, 137–138

ISMS (Information Security Management Systems), 44
incident management and, 579–580
ISO/IEC 27000 suite of information security standards, 12–15

ISO (International Organization for Standardization)
ISO 7498–4, Open Systems Interconnection-Basic Reference Model-Part 4: Management Framework, 393
ISO 22301, BCM methodology, 623
ISO 27002, Code of Practice for Information Security Controls, 162, 386
ISO 27005, information security risk management, 81–84

ISO 29100, 192
ISO/IEC 27000 suite of information security standards, 12–13
ISMS, 13–15
ISO 27001, 14, 15–16
ISO 27002, 14, 17–18
ISO 27005, 15
ISO 27014, 15
ISO 27036, 15
mapping to ISF SGP, 18–21

ISS (Information Security Steering) committees
COBIT 5, 64
ISS committees, 65

IT (Information Technology), 45

IT managers, ISS committees, 65

IT strategic planning, 48

IT systems, ICS versus, 225–228

ITSM (IT Service Management), SLA, 379

ITU (International Telecommunication Union), ITU-T security documents, 32–34, 45, 393

J - K

job descriptions, hiring process security, 164

key life cycle, 534–536

keyloggers, 91, 488

kill chains
defined, 96
phases of, 96–97

kits (virus generators), 91, 488

knowledge factor (user authentication), 310

KPI (Key Performance Indicators), 455

https://t.me/learningnets

L

labeling, information, 185
leakage of information. *See* DLP (Data Loss Prevention)
least privilege
defined, 230
human resource security, 165
level of risk, 76–77
likelihood (risk assessment)
defined, 76
determining risk, 77
likelihood assessments, 116–118
limited reliance on key employees, human resource security, 165
liveness detection, biometric authentication, 340
local environment security
best practices, 619
coordinating, 604–606
defined, 602–603
information protection champions, 605–606
information security coordinators, 604–605
physical security
best practices, 619
controls, 615–616
controls, assessments, 618–619
controls, baselines, 617–618
defense in depth strategies, 610–612
defined, 606
PSO, 609–610
security maps, depth of security, 611–612
threats, 606
threats, environmental threats, 607–608, 612–614
threats, human-caused physical threats, 609, 615
threats, preventing/mitigating, 612–615
threats, technical threats, 608–609, 614–615
profiles, 603–604
security champions, 605–606
local storage. *See* DAS
location services, security, 237
logic bombs, 90, 488
logs
defined, 556
log management policy, 558–559
network device logs, 557
office equipment threats/vulnerabilities, 218
OS logs, 557
security audits, 671–672
security event logs, 554–556
determining what to log, 557
log management policy, 558–559
objective of, 556
potential log sources, 556–557
securing data, 557–558
vulnerability logs, 551
web server logs, 557
lookup secrets, biometric authentication, 345
loss event frequency, 121–122

M

MaaS (Malware as a Service), 488
MAC (Mandatory Access Control), 349
machine learning, non-malware attacks, 577
machine-human interface, ICS, 225
mailboxes (MFD), office equipment threats/vulnerabilities, 218
maintenance
ICS, 225
remote network maintenance, 429–430
malicious behavior (culture of security), 168–169
malware
adware, 487
auto-rooters, 488
backdoors (trapdoors), 488
best practices, 541
bots (zombies), 489
clickless malware, 490
defined, 90, 487
downloaders, 488
droppers, 488

https://t.me/learningnets

exploits, 488
fileless malware, 490
flooders, 488
keyloggers, 488
kits (virus generators), 488
logic bombs, 488
MaaS, 488
malware protection software
capabilities of, 494–495
managing, 495–496
mobile codes, 488
nature of, 490
non-malware attacks, 576–577
polymorphic droppers, 488
practical malware protection, 490–494
PUP, 488, 490
ransomware, 489
RAT, 489
rootkits, 489
scrapers, 489
spammer programs, 489
spyware, 489
Trojan horses, 489
types of, 487–489
virus generators (kits), 488
viruses, 489
web drive-bys, 489
worms, 489
zombies (bots), 489
management phase (HAM), 215–216
management protocols, office equipment, 217
managing
applications. *See* AM
authentication management, ICS, 230
capacity, 383–384
change, 169, 386–389
CMDB, 212
configurations
defined, 139
ICS, 230
security management and, 139
cybersecurity, 34–37
documents, 198–202
information, 178–179
best practices, 205–206
classifying information, 179–185
document/records management, 198–204
handling information, 186
privacy, 186–198
security, 43–44
sensitive information, 204–205
log management policy, 558–559
malware protection software, 495–496
passwords, automated password managers, 314
patches, 230, 551–554
people
best practices, 175–176
human resource security, 160–166
security awareness/education, 166–175
performance, 383–384
physical assets, 210–211
best practices, 244–245
CMDB, 212
HAM, 211–212
HAM, acquisition phase, 214
HAM, average life cycle duration of common hardware, 216
HAM, deployment phase, 214–215
HAM, disposition phase, 216
HAM, management phase, 215–216
HAM, planning phase, 213–214
mobile devices, EMM systems, 242–243
mobile devices, enterprise infrastructures, 242–243
mobile devices, network protocols/services, 241–242
mobile devices, physical access, 242
mobile devices, security, 238–239, 243
mobile devices, technology stacks, 239–240
mobile devices, threats/vulnerabilities, 236–237
mobile devices, vetting applications, 240–241
office equipment, 217

https://t.me/learningnets

office equipment, threats/vulnerabilities, 217–219
resources, 243
PKI, 540–541
records/documents, 198–200, 202–204
risk, 80
defined, 76
ISO 27005 information security risk management, 81–84
NIST risk management framework, 179–183
security management and, 139
X.1055 risk management process, 80–81
security, 137
awareness/training, 138
best practices, 154
capacity planning, 138
CISO, role in, 137, 138–140
configuration management, 139
consistency in security, 139
contingency planning, 139
external requirements function, 140
governance, 138
incident response, 139
ISM, role in, 137–138
monitor function, 140
performance measures, 139
planning, 138
policies, 151
products/services acquisition, 138
projects function, 140
risk management and, 139
support function, 139
system development life cycle, 138
sensitive information, 204–205
system development, 273–274
environments, 275–277
methodologies, 274–275
QA, 277

mandatory vacations, human resource security, 165

man-in-the-middle attacks, VoIP, 443

MDA (Mail Delivery Agents), 432

memorized secrets, biometric authentication, 345

memory cards, user authentication, 322–323

methodologies of system development, 274–275

MFA (Multifactor Authentication), 230

MFD (Multifunction Devices). *See also* office equipment, 217

address books, threats/vulnerabilities, 218
cryptographic erasure, 222–223
equipment disposal, 222–223
logs, threats/vulnerabilities, 218
mailboxes, threats/vulnerabilities, 218
management protocols, 217
OS security, 219
physical security, 219
security controls, 219–222
SED, 222
services protocols, 217–218
threats/vulnerabilities, 217
DoS attacks, 218–219
information disclosure, 218
network services, 217–218

mirroring ports, 511

misuse detection (intrusion detection), 504

mobile codes, 91, 488

mobile devices

applications, vetting, 240–241
cloud-based applications, 232
de-perimeterization, 232
ecosystem of, 234–236
EMM systems, 242–243
enterprise infrastructures, 242–243
network management, 416
network protocols/services, 241–242
physical access, 242
resources, 243
screen locks, 242
security, 231–233, 243
security strategies, 238–239
technology stacks, 233–234, 239–240
threats/vulnerabilities, 236–237

https://t.me/learningnets

ModSecurity WAF (Web Application Firewall), 293
money flows (supply chains), 451
monitoring
active monitoring, 511–512
ICS security, 231
passive monitoring, 511–512
password use, 314
monitoring security
best practices, 691–692
security audit trails
application-level audit trails, 671
defined, 667
network-level audit trails, 671
physical access audit trails, 671–672
system-level audit trails, 671
user-level audit trails, 671
security audits
controls, 673–677
data collection, 668–672
defined, 666–667
elements of, 668
external audits, 672–673
internal audits, 672
logs, 671–672
objectives of, 667
security management, 140
security performance, 678
compliance monitoring, 690–691
metrics, 678–679
metrics, defined, 682–683
metrics, development process, 683–685
metrics, examples of, 680–681
metrics, monitoring/reporting, 686–688
metrics, risk reporting, 688–689
metrics, sources of, 679–680
metrics, values of, 682
monitoring/reporting, 686–688
risk reporting, 688–689
security policies, 151–152
MS (Message Stores), 432
MSA (Mail Submission Agents), 432
MSP (Managed Service Providers), SLA, 379
MTA (Message Transfer Agents), 432
MTD (Maximum Tolerable Downtime), 632
MUA (Message User Agents), 431–432
multifactor authentication, 311–312
multiple password use, exploiting, 314

N

NAP (Network Access Points), physical network management, 423
NAS (Network Attached Storage), 378–379
National Science Foundation, 210
native virtualization, 371–372, 373
natural disasters
BCM, 626
local environment security, 607–608, 612–614
negligent behavior (culture of security), 168
nested (hosted) virtualization, 372
network management, 393
accounting management, 393, 395–396
best practices, 444–445
configuration management, 393, 396–397
device logs, 557
DMZ, defined, 508
DMZ networks, 414–416
documentation, physical network management, 423
external network connections, 427–428
fault management, 393, 394–395
firewalls, 292, 404
characteristics of, 404–405
DMZ networks, 414–416
limitations of, 406
next-generation firewalls, 414
packet filtering firewalls, 406–411
planning, 428–429
policies, 428
stateful inspection firewalls, 411–413
stateful inspection firewalls, application-level gateways, 413
stateful inspection firewalls, circuit-level

https://t.me/learningnets

gateways, 413–414
VPN (firewall-based), 420
IPSec, 418–420
mobile devices, 416
network management systems
architecture of, 402–404
components of, 399–401
distributed network management systems, 401–402
element management layer, 403
NME, 400–401
NML, 403–404
service management layer, 404
performance management, 393, 397–398
physical network management, 423–426
NAP, 423
network documentation, 423
telecommunication cables, 423
providers, SLA, 379–381
remote network maintenance, 429–430
SDN, defined, 85
security, 4
device configuration, 421–423
managing, 393, 398–399
services, office equipment threats/vulnerabilities, 217–218
storage, 377
DAS, 377
NAS, 378–379
SAN, 377–379
VoIP networks, 438
context, 440–442
processing, 439–440
security, 443
signaling, 439
threats, 442–443
VPN, 417–418, 426–427
defined, 241
external network connections, 428
firewall-based VPN, 420
VoIP networks, 443
WAP, 416
wireless network management, 416–417
wireless network security, 426–427

next-generation firewalls, 414

NFV (Network Function Virtualization), 85

NIDS (Network-based Intrusion Detection Systems), 503, 506

cyber attack kill chains, 575
deploying, 507–508
function of, 506

NIST (National Institute of Standards and Technology), 188

ATE, 172
cybersecurity framework and security documents, 21–22, 25–26
components of, 22–25
FIPS 200, 26
FIPS 800-27, 26
SP 800-12, 26
SP 800-55, 26
SP 800-100, 26
SP 800-144, 26
SP 1800, 26
NVD, 103–104
CVSS metrics, 105–107
scoring example, 104–105
risk management framework, 179–183
SDLC, 248–249
development/acquisition phase, 250–251, 264–266
disposal phase, 252, 272–273
implementation/assessment phase, 251–252, 266–270
incorporating security, 259–260
incorporating security, development/acquisition phase, 264–266
incorporating security, disposal phase, 272–273
incorporating security, implementation/assessment phase, 266–270
incorporating security, initiation phase, 260–263
incorporating security, operations/maintenance phase, 270–272

https://t.me/learningnets

initiation phase, 249–250
initiation phase, security, 260–263
operations/maintenance phase, 252, 270–272
SP 800-12, 26
SP 800-16, 166
SP 800-18, 140–141
SP 800-37, 261, 267–269
SP 800-41, 428
SP 800-45, 434
SP 800-50, 166
SP 800-53, 63, 196–198
SP 800-53A, 267–269
SP 800-55, 26
SP 800-63, 307–310
SP 800-63B, 321, 340–341
SP 800-88, 272
SP 800-90A, 321
SP 800-100, 26
SP 800-122, 198
SP 800-125, 374–376
SP 800-125A, 374–375
SP 800-144, 26
SP 800-162, 357–358
SP 800-177, 433
SP 800-178, 358
SP 1800, 26
SP 1800-3, 358
NISTIR 7874, 358–360
NISTIR 8112, 358
NME (Network Management Entities), 400–401
NML (Network Management Layer), network management systems, 403–404
noise (EMI), 609
non-malware attacks, 576–577
nonrepudiation, 5
NTP (Network Time Protocol), 594
number generators (pseudorandom), 535
NVD (National Vulnerability Database), 103–104
CVSS metrics, 105–107
scoring example, 104–105

O

objects (system access), 348
office equipment, security. *See also* MFD, 217
address books, threats/vulnerabilities, 218
cryptographic erasure, 222–223
equipment disposal, 222–223
logs, threats/vulnerabilities, 218
mailboxes, threats/vulnerabilities, 218
management protocols, 217
OS security, 219
physical security, 219
security controls, 219–222
SED, 222
services protocols, 217–218
threats/vulnerabilities, 217
DoS attacks, 218–219
information disclosure, 218
network services, 217–218
offline dictionary attacks, 313
Open Group security standards, 114–115
Open Web Application Security Project, application security risks, 290–291
operating characteristic curves, biometric authentication, 336
operations/maintenance phase (NIST SDLC), 252, 270–272
organizational information/decision work flows, cybersecurity management process, 36–37
ORR (Operational Readiness Reviews), 270
OS (Operating Systems)
logs, 557
mobile OS, 234
security, office equipment, 219
OTP (One-Time Password) devices, 328–329, 345
outages (power), 608
overvoltage, 609
OWASP (Open Web Application Security Project)
Risk Rating Methodology, 294
Testing Guide, 295
ownership, total cost of (TCO), 281–283

https://t.me/learningnets

P

PaaS (Platform as a Service), 468, 472
PACE (Password Authentication Connection Establishment), 327
packet filtering firewalls, 406–411
Packet Storm, vulnerability management, 549
PAD (Presentation Attack Detection), 339–340
parallel runs, implementation/assessment phase (NIST SDLC), 252
partial document matching, 510
passive monitoring, 511–512
passwords, 312
automated password managers, 314
blacklists, 321
cracking, 317–319
discretionary access control, 312
file access control, 319–320
guessing, 313
hashed passwords, 315–316
monitoring, 314
multiple password use, exploiting, 314
offline dictionary attacks, 313
OTP devices, 328–329, 345
PACE, 327
password attacks
defined, 92
popular password attacks, 313
regulating password selection, 321
shadow password files, 319
specific account attacks, 313
system-selected passwords, 321–322
UNIX password schemes, 315–316
user-selected passwords, 320
vulnerabilities, 313–315
workstation hijacking, 313
patches
cyber attack kill chains, 574
ICS
patch management, 230
patch vulnerability, 228–229
managing, 551–554
virtual patching, ModSecurity WAF, 293
PCI (Payment Card Industry), PCI-DSS, 30–32
penetration testing, 265
people management
best practices, 175–176
human resource security, 160–162
current employees, 164–165
dual operator policies, 165
hiring process, 162
hiring process, background checks/screening, 162–163
hiring process, directory servers, 164
hiring process, employment agreements, 163
hiring process, job descriptions, 164
limited reliance on key employees, 165
privileges, 165
remote working, 176
separation of employee duties, 165
termination of employment, 165–166
vacations, 165
security awareness/education, 166, 168
awareness program communication materials, 170–172
awareness program evaluation, 172
certification, 174–175
culture of security, 168
cybersecurity essentials program, 173
cybersecurity learning continuum, phases of, 167
NIST ATE, 172
processes of, 169–170
role-based training, 173–174
SP 800-16, 166
SP 800-50, 166
performance, 393, 397–398
APM, 285–286
business continuity readiness, evaluating performance, 650–653
internal audits, 653–654
management reviews, 654
managing, 383–384
performance measures and security management, 139
security performance, 678

https://t.me/learningnets

compliance monitoring, 690–691
metrics, 678–679
metrics, defined, 682–683
metrics, development process, 683–685
metrics, examples of, 680–681
metrics, monitoring/reporting, 686–688
metrics, risk reporting, 688–689
metrics, sources of, 679–680
metrics, values of, 682
monitoring/reporting, 686–688
risk reporting, 688–689
phishing
defined, 92, 565
spear phishing, defined, 571
physical asset management, 210–211
best practices, 244–245
CMDB, 212
HAM, 211–212
acquisition phase, 214
average life cycle duration of common hardware, 216
deployment phase, 214–215
disposition phase, 216
management phase, 215–216
planning phase, 213–214
ICS
defined, 223
elements of, 224–225
IT systems versus, 225–228
security, 227–228, 229–231
threats/vulnerabilities, 228–229
mobile devices
ecosystem of, 234–236
EMM systems, 242–243
enterprise infrastructures, 242–243
network protocols/services, 241–242
physical access, 242
resources, 243
security, 231–233, 243
security strategies, 238–239
technology stacks, 233–234, 239–240
threats/vulnerabilities, 236–237
vetting applications, 240–241
office equipment, 217
cryptographic erasure, 222–223
equipment disposal, 222–223
OS security, 219
physical security, 219
security controls, 219–222
threats/vulnerabilities, 217–219
physical network management, 423
NAP, 423
network documentation, 423
telecommunication cables, 423
TIA-492, 423–426
physical security
best practices, 619
controls, 615–616
assessments, 618–619
baselines, 617–618
defense in depth strategies, 610–612
defined, 606
PSO, 609–610
security maps, depth of security, 611–612
threats, 606
environmental threats, 607–608, 612–614
human-caused physical threats, 609, 615
preventing/mitigating, 612–615
technical threats, 608–609, 614–615
PII (Personally Identifiable Information), 112, 261–262
pilot runs, implementation/assessment phase (NIST SDLC), 252
PKI (Public Key Infrastructure), 536
architecture of, 538–540
best practices, 542
CA, 539–540
managing, 540–541
public key certificates, 536–538
RA, 539
relying parties, 539–540
repositories, 539
planning
capacity planning, 138
capital planning, security planning, 142–145
changes, change management, 387

https://t.me/learningnets

contingency planning and security management, 139
firewall implementations, 428–429
security planning, 138
capital planning, 142–145
defined, 140
example of, 141–142
process of, 141–142
requirements, 142
security policies, 145
security policies, AUP, 146, 152–153
security policies, categories of, 146–147
security policies, information security strategic planning, 146
security policies, managing, 151
security policies, monitoring, 151–152
security policies, Router and Switch Security Policy (SANS Institute), 148–150
security policies, security-related documents, 145–146
security policies, templates, 147–150
SP 800-18, 140–141
strategic planning, 47
defined, 47
enterprise strategic planning, 47
framework of, 51–52
information security strategic planning, 50
IT strategic planning, 48

planning phase (HAM), 213–214

POA&M (Plans of Action and Milestones), 269, 272

policies

AUP, 146, 152–153
email, 434–435
IM, 436–437
SANS Institute AUP template, 152–153
BYOD policies, 173
dual operator policies, human resource security, 165
firewall policies, 428
incident management policies, 580–581
log management policy, 558–559
privacy policies
COPPA, 195
Electronic Communications Privacy Act, The, 195
FACTA, 195
Federal Policy for the Protection of Human Subjects, 195
FERPA, 195
GDPR, 193–195
GLBA, 195
HIPAA, 195
ISO 29100, 192
Privacy Act of 1974, The, 195
Router and Switch Security Policy (SANS Institute), 148–150
security policies, 145
AUP, 146, 152–153
categories of, 146–147
defined, 9
IM, 437–438
information security strategic planning, 146
managing, 151
monitoring, 151–152
NIST SP 800-53, 63
security-related documents, 145–146
templates, 147–150

polymorphic droppers, 488

popular password attacks, 313

port administration, VoIP networks, 443

port mirroring, 511

portfolio management practices (APFM), 284–285

possession factor (user authentication), 310

possession-based authentication. *See* hardware tokens

power outages (undervoltage), 608

PowerShell, 576

presentation attacks, 339–340

print logs, office equipment threats/vulnerabilities, 218

privacy

information management, 186–188
Chase Bank online privacy policy, 190
collecting information, 189

https://t.me/learningnets

disseminating information, 190–191
Google privacy policy, 190
invasions, 190–191
principles/policies, 191–198
privacy controls, 196–198
processing information, 189–190
security's relationship to privacy, 188
threats to privacy, 189–191
U.S. privacy laws/regulations, 195
principles/policies
COPPA, 195
Electronic Communications Privacy Act, The, 195
FACTA, 195
Federal Policy for the Protection of Human Subjects, 195
FERPA, 195
GDPR, 193–195
GLBA, 195
HIPAA, 195
ISO 29100, 192
Privacy Act of 1974, The, 195
Privacy Act of 1974, The, 195
threats to privacy
aggregation, 190
appropriation, 191
blackmail, 191
breach of confidentiality, 190
decisional interference, 191
disclosure, 190
distortion, 191
exclusion, 190
exposure, 190
identification, 190
increased accessibility, 191
insecurity, 190
interrogation, 189
intrusion, 191
secondary use, 190
surveillance, 189
private clouds, 468–469
privileges
elevation of privileges, 90
human resource security, 165
least privilege, 230
PRM (Performance Reference Models), 60
processing information, threats to privacy, 189–190
product/service flows (supply chains), 450
projects function, security management, 140
pseudorandom number generators, 535
PSO (Physical Security Officers), 609–610
public clouds, 468, 469–470
public key encryption, 520–521
PUP (Potentially Unwanted Programs), 488, 490

Q

QA (Quality Assurance), system development, 277
qualitative risk assessment, 108–110, 111–112
quantitative risk assessment, 107–108, 109–110

R

RA (Registration Authorities), 539
RACI charts, security governance, 66–67
ransomware, 90, 489
RAT (Remote Access Trojans), 489
RBAC (Role-Based Access Control), 349, 351–353
real-time antivirus software, VoIP networks, 443
records management, 198–200, 202–204
recovery/restoration plans, 646–647, 657–659
reengineering, APFM, 284
reliance on key employees, human resource security, 165
relying parties (PKI), 539–540
remote access attacks, 92
remote access security, ICS, 230
remote diagnostics, ICS, 225
remote network maintenance, 429–430

https://t.me/learningnets

remote working, 176
reports
risk assessment reports, 92–93
Cisco Annual Cybersecurity Reports, 98
ENISA Threat Landscape Reports, 95–96
Fortinet Threat Landscape Reports, 98
Threat Horizon Reports, 94–95
Trustwave Global Security Reports, 97
Verizon DBIR, 93–94
risk reporting (security performance), 688–689
vulnerability reports, 551
repositories (PKI), 539
repudiation threats, 89
requirements, security planning, 142
residual risk, 76
responsive controls, 101
reverse proxy servers
defined, 293
ModSecurity WAF, 293
RFID (Radio Frequency Identification) tags, 185
risk
avoidance, 130–131
criteria, defined, 76
CRO, security governance, 55
defined, 4, 76
determination, 128
ERM committees, 65
evaluating, 76, 128–129
identifying, 76
level of risk, defined, 76–77
managing, 76, 80
ISO 27005 information security risk management, 81–84
NIST risk management framework, 179–183
SCRM, 453–456
security management and, 139
X.1055 risk management process, 80–81
reducing, 130
reporting (security performance), 688–689
retention/acceptance, 130
transferring, 131
treatments, defined, 76
risk analysis
defined, 76
events, threat event frequency, estimating, 118–119
FAIR, 114, 115–116
BIRT, 126–127
impact assessment, 122–123
likelihood assessments, 116–118
loss estimation, 123–126
loss event frequency, 121–122
Open Group security standards, 114–115
risk assessment matrices, 120–121
risk avoidance, 130–131
risk determination, 128
risk evaluation, 128–129
risk retention/acceptance, 130
risk transfer, 131
risk treatment, 129–130
simple risk analysis worksheet, 113–114
risk assessment, 74–75, 78, 80
assets
asset register, 87–88
business assets, 87
defined, 75, 77
determining future problems, 79
hardware assets, 85
identifying, 84–85
information assets, 86–87
software assets, 85
BCM, 632–634
best practices, 131–132
biometric authentication, 340–341
cloud computing, 475–476
container virtualization, defined, 85
control identification, 98–99
avoidance controls, 100
checklist of controls, 101–102
deterrent controls, 100–101
online catalog of security controls, 99–100
responsive controls, 101
vulnerability controls, 101
costs of, 108
defined, 76

https://t.me/learningnets

EUDA, 296–297
events
  defined, 75
  threat event frequency, estimating, 118–119
FAIR, 114, 115–116
  BIRT, 126–127
  impact assessment, 122–123
  likelihood assessments, 116–118
  loss estimation, 123–126
  loss event frequency, 121–122
  Open Group security standards, 114–115
  risk assessment matrices, 120–121
impact
  defined, 75
  determining risk, 77
level of risk, defined, 76–77
likelihood
  defined, 76
  determining risk, 77
likelihood assessments, 116–118
NFV, 85
OWASP Risk Rating Methodology, 294
PII, 112
qualitative risk assessment, 108–110, 111–112
quantitative risk assessment, 107–108, 109–110
reports, 92–93
  Cisco Annual Cybersecurity Reports, 98
  ENISA Threat Landscape Reports, 95–96
  Fortinet Threat Landscape Reports, 98
  Threat Horizon Reports, 94–95
  Trustwave Global Security Reports, 97
  Verizon DBIR, 93–94
residual risk, defined, 76
RoE, 76
SDN, defined, 85
security categories, 110–111
security control, defined, 76
security incidents, defined, 76
terminology of, 75–76
threat actions, defined, 75
threat agents, defined, 75
threats, 89
adware, 91
auto-rooters, 91
backdoors (trapdoors), 91
business resource threats, 89
classifying, 89–90
code injection, 92
data tampering, 89
DDoS attacks, 92
defined, 75, 76
determining future problems, 79
determining risk, 77
DNS attacks, 92
DoS attacks, 90, 92
downloaders, 91
droppers, 91
elevation of privileges, 90
environmental threats, 89
exploit kits, 91
exploits, 91
flooders, 91
hackers (crackers), 92
hostile actors, 89
identifying, 89
information disclosure, 90
injection flaws, 92
keyloggers, 91
logic bombs, 90
malware, 90
mobile codes, 91
password attacks, 92
phishing, 92
ransomware, 90
remote access attacks, 92
repudiation threats, 89
rootkits, 91
social engineering, 92
spam, 90
spammer programs, 91
spoofing identity, 89
spyware, 91
STRIDE threat model, 89–90
threat event frequency, estimating, 118–119

https://t.me/learningnets

Trojan horses, 91
virus generators (kits), 91
viruses, 90
website exploits, 92
worms, 90
zombies (bots), 91
value proposition, defined, 123
VM, defined, 84
vulnerabilities
categories of, 103
defined, 76
determining future problems, 80
determining risk, 78
estimating, 119–120
identifying, 102
NVD, 103–104
RM (Reference Models)
ARM, 60–61
assets of, 62
BRM, 60
DRM, 60
enterprise architecture RM, 59–62
IRM, 61
PRM, 60
relationships between components, 61
SRM, 61–62
RoE (Risk of Exposure), 76
rogue AP (Access Points), wireless network security, 427
role-based training, security awareness/education, 173–174
rootkits, 91, 489
Router and Switch Security Policy (SANS Institute), 148–150
RPO (Recovery Point Objectives), 632
RTO (Recovery Time Objectives), 632
rule-based recognition (DLP), 509

S

S/MIME, 433
SaaS (Software as a Service), 467–468
SABSA (Sherwood Applied Business Security Architecture), 483–487
SAN (Storage Area Networks), 377–379
SANS Institute
AUP template, 152–153
computer security training and certification, 175
Router and Switch Security Policy, 148–150
scanning for vulnerabilities, 549–551
SCM (Supply Chain Management), 449
best practices, 478–479
elements of, 451–452
flows, 450–451
ICT supply chains
defined, 449
flows, 450–451
SCRM, 453–456
SCRM, threats, 456–459
SCRM, 453–456
best practices, 463–466
exfiltration, 457
IPR, 455
KPI, 455
security controls, 460–463
threats, 456–459
vulnerabilities, 459–460
security controls, 460–463
supply chains, defined, 449
threats, 456–459
vulnerabilities, 459–460
scrapers, 489
screen locks (mobile devices), 242
screening employees/background checks, 162–163
SCRM (Supply Chain Risk Management), 453–456
best practices, 463–466
exfiltration, defined, 457
IPR, 455
KPI, 455
security controls, 460–463
threats, 456–459
vulnerabilities, 459–460

https://t.me/learningnets

SDLC (System Development Life Cycle), 248–249
NIST SDLC
development/acquisition phase, 250–251
development/acquisition phase, security, 264–266
disposal phase, 252
disposal phase, security, 272–273
implementation/assessment phase, 251–252
implementation/assessment phase, security, 266–270
incorporating security, 259–260
incorporating security, development/acquisition phase, 264–266
incorporating security, disposal phase, 272–273
incorporating security, implementation/assessment phase, 266–270
incorporating security, initiation phase, 260–263
incorporating security, operations/maintenance phase, 270–272
initiation phase, 249–250
initiation phase, security, 260–263
operations/maintenance phase, 252
operations/maintenance phase, security, 270–272
SGP SDLC, 253–254
SDN (Software-Defined Networking), 85
secondary use, privacy threats, 190
secrets, biometric authentication, 345
secure hash functions, 522–524
security
accreditation. *See* authorization
applications, 237, 287
business application registers, 287–288
external application security, 289
internal application security, 288–289
web applications, 293
web applications, policies, 294–295
web applications, risks, 289–291
web applications, WAF, 291–293
authorization, 270
implementation/assessment phase (NIST SDLC), 269
operations/maintenance phase (NIST SDLC), 272
awareness/education, 166, 168
awareness program communication materials, 170–172
awareness program evaluation, 172
certification, 174–175
culture of security, 168
cybersecurity essentials program, 173
cybersecurity learning continuum, phases of, 167
NIST ATE, 172
processes of, 169–170
role-based training, 173–174
SP 800-16, 166
SP 800-50, 166
categories of, 110–111
classification process, information management, 183–185
cloud computing, 473
cloud-based applications, 232
risk assessment, 475–476
threats, 474–475
contingency training, 267–269
controls
defined, 15, 76
office equipment, 219–222
SCRM, 460–463
customer data, 361
EUDA security framework, 297–300
event logs, 554–556
determining what to log, 557
log management policy, 558–559
objective of, 556
potential log sources, 556–557
securing data, 557–558
firewalls, 404
application-layer firewalls, VoIP networks, 443
characteristics of, 404–405

https://t.me/learningnets

cyber attack kill chains, 574
limitations of, 406
network-based firewalls, 292
planning, 428–429
policies, 428
WAF, 291–293, 574
governance, 138
best practices, 69–70
CEO, 55
CIO, 55
CISO, 55
components of, 47
COO, 55
CPO, 55
CRO, 55
CSO, 55
defined, 43
desired outcomes, 46
effectiveness of, 68–69
enterprise architecture integration, 58
evaluating, 68–69
framework of, 63
information security architectures, 58
information security governance, defined, 42–43
ISMS, 44
principles of, 45–46
reporting relationships for, 56
roles/responsibilities of, 55, 57–58
security direction, 64–67
security management and, 138
security programs, defined, 43
stakeholders, defined, 45–46
strategic planning, 47, 48–50, 51–52
GPS (location services), 237
human resource security, 160–162
current employees, 164–165
dual operator policies, 165
hiring process, 162
hiring process, background checks/screening, 162–163
hiring process, directory servers, 164
hiring process, employment agreements, 163
hiring process, job descriptions, 164
limited reliance on key employees, 165
privileges, 165
remote working, 176
separation of employee duties, 165
termination of employment, 165–166
vacations, 165
hypervisors, 376
IM security policy, 437–438
incidents, defined, 76
information security, 4, 68–69
COBIT 5, 29–30, 64–66
information security architectures, 58
information security governance, defined, 42–43
information security management, defined, 43
information security reports, 53–55
information security strategic planning, 50
ISMS, 44
ISO/IEC 27000 suite of information security standards, 12–21
Standard of Good Practice for Information Security (SGP), 9–12
location services, 237
managing, 137, 393, 398–399
awareness/training, 138
best practices, 154
capacity planning, defined, 138
CISO, role in, 137, 138–140
configuration management, 139
consistency in security, 139
contingency planning, 139
external requirements function, 140
incident response, 139
ISM, role in, 137–138
monitor function, 140
performance measures, 139
projects function, 140
risk management and, 139
security governance, 138

https://t.me/learningnets

security planning, defined, 138
security products/services acquisition, 138
support function, 139
system development life cycle, 138
maps, depth of security, 611–612
mobile devices, 231–233, 238–239
network management, device configuration, 421–423
network security, 4
NIST SDLC, 259–260
development/acquisition phase, 264–266
disposal phase, 272–273
implementation/assessment phase, 266–270
initiation phase, 260–263
operations/maintenance phase, 270–272
planning
capital planning, 142–145
defined, 138, 140
example of, 141–142
process of, 141–142
requirements, 142
security policies, 145–150, 151–153
SP 800-18, 140–141
policies. *See* policies
privacy's relationship to security, 188
programs, defined, 43
servers, requirements, 368–370
technical security management, security architectures, 483–487
virtualization
hypervisors, 376
issues with security, 374–375
VoIP networks, 443
wireless network security
hackers (crackers), 427
VPN, 426–427

Security Accreditation Packages, 269

security champions, 605–606

security incident management frameworks, 577–578

best practices, 597–598
emergencies, handling, 590–592
forensics, 592–593
collection phase, 594–595
identification phase, 594
preparation phase, 593–594, 595–596
preservation phase, 595
reporting phase, 596
gathering information, 583
incident handling checklist, 589
incident response process, 584–585
containment/eradication/recovery phase, 587–588
detection/analysis phase, 586–587
incident handling checklist, 589
post-incident activity phase, 588–589
preparation phase, 585
ISMS and, 579–580
objectives of, 579
policies, 580–581
resources, 578–579
roles/responsibilities of, 581–582
tools, 583–584

security monitoring

best practices, 691–692
security audit trails
application-level audit trails, 671
defined, 667
network-level audit trails, 671
physical access audit trails, 671–672
system-level audit trails, 671
user-level audit trails, 671
security audits
controls, 673–677
data collection, 668–672
defined, 666–667
elements of, 668
external audits, 672–673
internal audits, 672
logs, 671–672
objectives of, 667
security performance, 678
compliance monitoring, 690–691
metrics, 678–679

https://t.me/learningnets

metrics, defined, 682–683
metrics, development process, 683–685
metrics, examples of, 680–681
metrics, monitoring/reporting, 686–688
metrics, risk reporting, 688–689
metrics, sources of, 679–680
metrics, values of, 682
monitoring/reporting, 686–688
risk reporting, 688–689
SecurityFocus, vulnerability management, 549
SED (Self-Encrypting Drives), 222
SEM (Security Event Management), 559–560
assessing security, 562–563
best practices, 561–563
deploying, 563
functions of, 560–561
planning, 561–562
simplifying security, 563
sensitive information
defined, 171–172
managing, 204–205
sensors, ICS, 224
separation of duties, human resource security, 165
servers. *See also* virtualization
directory servers, defined, 164
DoS attacks, 368
reverse proxy servers
defined, 293
ModSecurity WAF, 293
security, requirements, 368–370
threats to, 368
web server logs, 557
service management layer (network management systems), 404
services protocols, office equipment, 217–218
SGP (Standard of Good Practice for Information Security), 7–10
areas of, 10–12
categories of, 10–12
environment security, 277
ISF SGP, security governance, 64
mapping ISO 27000 suite to ISF SGP, 18–21
SDLC, 253–254
shadow password files, 319
side-channel attacks, 242
SIEM (Security Information and Event Management), 569
signatures (digital), 518, 524–525
simple risk analysis worksheet, 113–114
single version of truth. *See* golden records
SLA (Service-Level Agreements), 379–381
cloud service providers, 382–383
CSIRT, 381–382
ITSM, 379
MSP, 379
smart cards, user authentication, 323–325
SOC (Security Operations Centers), 97
social engineering
defined, 92
social engineering attacks, defined, 571
software
antivirus software, cyber attack kill chains, 574
assets, defined, 85
COTS software, 288
real-time antivirus software, VoIP networks, 443
SDN, defined, 85
source code repositories, 263
source routing attacks, 411
SP 800-12, 26
SP 800-16, 166
SP 800-18, 140–141
SP 800-37, 261, 267–269
SP 800-41, 428
SP 800-45, 434
SP 800-50, 166
SP 800-53, 63, 196–198
SP 800-53A, 267–269
SP 800-55, 26
SP 800-63, 307–310
SP 800-63B, 321, 340–341
SP 800-88, 272
SP 800-90A, 321, 534

https://t.me/learningnets

SP 800-90B, 534
SP 800-90C, 534
SP 800-100, 26
SP 800-122, 198
SP 800-125, 374–376
SP 800-125A, 374–375
SP 800-144, 26
SP 800-162, 357–358
SP 800-177, 433
SP 800-178, 358
SP 1800, 26
SP 1800-3, 358
spam, 90
spammer programs, 91, 489
spear phishing, 571
specific account attacks, 313
SPF (Sender Policy Framework), 433
SPIT (Spam over Internet Telephone), 443
spoofing
biometric spoofing, 339
identity spoofing, 89
spyware, 91, 489
SRM (Security Reference Models), 61–62
SSCP (Systems Security Certified Practitioner), 175
SSID (Secure Set Identifiers), WAP, 426
SSO (Single Sign-On), 497
stakeholders, 45–46
Standard of Good Practice for Information Security (SGP), 7–10
areas of, 10–12
categories of, 10–12
mapping ISO 27000 suite to ISF SGP, 18–21
standards and best practices documents, 6–7, 36–37
CIS CSC, 27–28
COBIT 5 for information security, 29–30
ISO/IEC 27000 suite of information security standards, 12–13
ISMS, 13–15
ISO 27001, 14, 15–16
ISO 27002, 14, 17–18
ISO 27005, 15
ISO 27014, 15
ISO 27036, 15
mapping to ISF SGP, 18–21
ITU-T security documents, 32–34
NIST cybersecurity framework and security documents, 21–22, 25–26
components of, 22–25
FIPS 200, 26
FIPS 800-27, 26
SP 800-12, 26
SP 800-55, 26
SP 800-100, 26
SP 800-144, 26
SP 1800, 26
PCI-DSS, 30–32
Standard of Good Practice for Information Security (SGP), 7–10
areas of, 10–12
categories of, 10–12
mapping ISO 27000 suite to ISF SGP, 18–21
STARTTLS, 433
stateful inspection firewalls, 411–413
application-level gateways, 413
circuit-level gateways, 413–414
storage
DAS, 377
local storage. *See* DAS
NAS, 378–379
network storage, 377
DAS, 377
NAS, 378–379
SAN, 377–379
SAN, 377–379
strategic planning, 47
defined, 47
enterprise strategic planning, 47
framework of, 51–52
information security strategic planning, 50
IT strategic planning, 48
STRIDE threat model, 89–90
subjects (system access), 348
supply chains. *See* SCM (Supply Chain Management)

https://t.me/learningnets

support, security management, 139
surveillance, privacy threats, 189
switches, Router and Switch Security Policy (SANS Institute), 148–150
symmetric encryption, 518–520
system access
access control, 305, 347
ABAC, 349, 353–355
ABAC, attribute metadata, 355–357
ABAC, resources, 357–358
access rights, 348–349
ACL, 350–351
DAC, 349–351
discretionary access control, 312
MAC, 349
metrics, 358–360
objects, 348
RBAC, 349, 351–353
subjects, 348
authorization, 305, 306–307
best practices, 362–363
customer access
arrangements, 360
connections, 361
contracts, 361
data security, 361
defined, 360
defined, 305–306
functions of, 305
user authentication. *See* user authentication
system development
best practices, 278
environments, 275–277
managing, 273–274
environments, 275–277
methodologies, 274–275
QA, 277
methodologies, 274–275
NIST SDLC. *See* SDLC
QA, 277
security, contingency training, 267–269
SGP SDLC, 253–254
waterfall development, 249
system owners, 261
systems management
backups, 384–386
best practices, 389–390
capacity management, 383–384
change management, 386–389
cloud service providers, 382–383
CSIRT, 381–382
defined, 366–367
elements of, 366–367
network storage, 377
DAS, 377
NAS, 378–379
SAN, 377–379
performance management, 383–384
servers. *See also* virtualization
security requirements, 368–370
threats to, 368
SLA, 379–381
cloud service providers, 382–383
CSIRT, 381–382
ITSM, 379
MSP, 379
trust relationships, 369
virtualization. *See also* servers
container virtualization, 374
hosted (nested) virtualization, 372
hosted virtualization security, 377
hypervisors, 371
hypervisors, functions of, 371
hypervisors, security, 376
hypervisors, types of, 371–374
infrastructure security, 376
native virtualization, 371–372, 373
security, hosted virtualization security, 377
security, infrastructure security, 376
security, issues with, 374–375
VM, 370
system-selected passwords, 321–322

https://t.me/learningnets

T

tampering with data, 89
tarpits, cyber attack kill chains, 575
TCO (Total Cost of Ownership), 281–283
technical security management
best practices, 541–542
cryptography. *See* cryptography
defined, 482–483
DLP, 509
classifying data, 509–510
data at rest, 510–511
data in motion (or transit), 510, 511–512
data in use, 510, 512
database fingerprinting, 509
exact file matching/hash values, 510
partial document matching, 510
rule-based recognition, 509
DRM, 512
architecture of, 514–515
best practices, 515–517, 542
components of, 513–514
IAM, 496
architecture of, 497–498
best practices, 501–502, 542
defined, 496
federated identity management, 498–500
planning, 500–501
SSO, 497
intrusion detection, 502, 504
anomaly detection, 504–505
best practices, 508–509, 542
false negatives, 504–505
false positives, 504–505
HIDS, 503, 505–506
IDS, 502–503, 508–509
misuse detection, 504
NIDS, 503, 506–508
principles of, 503–504
true negatives, 505
true positives, 505
malware
best practices, 541
defined, 487
malware protection software, 494–496
nature of, 490
practical malware protection, 490–494
types of, 487–489
PKI, 536
architecture of, 538–540
best practices, 542
CA, 539–540
managing, 540–541
public key certificates, 536–538
RA, 539
relying parties, 539–540
repositories, 539
SABSA, 483–487
security architectures, 483–487
technical controls, defined, 482–483
technical threats
BCM, 627
local environment security, 608–609, 614–615
technical vulnerability management. *See* vulnerabilities
technology stacks
applications, 234
firmware, 234
mobile devices, 239–240
mobile OS, 234
telecommunication cables, physical network management, 423
telephony (IP)/conferencing, 443–444
templates (AUP), 152–153
termination of employment, human resource security, 165–166
tests
business continuity readiness, 647–648, 649–650
end-user testing, defined, 265
functional testing, defined, 265
integration testing, 251
OWASP Testing Guide, 295
penetration testing, defined, 265
UAT, 251
user testing, defined, 265

https://t.me/learningnets

theft of service, VoIP, 443
threat actions, 75
threat agents, 75
Threat Horizon Reports, 94–95
Threat Landscape Reports, 95–96
threats, 89
adware, defined, 91
analyzing, 569–570
APT, defined, 566
auto-rooters, defined, 91
backdoors (trapdoors), defined, 91
BCM
environmental threats, 627
human-caused physical threats, 627–628
natural disasters, 626
system problems, 627
business resource threats, defined, 89
classifying, 89–90
code injection, defined, 92
data tampering, 89
DDoS attacks, defined, 92
defined, 5, 75–76
determining risk, 77
DNS attacks, defined, 92
DoS attacks, 90, 92
downloaders, defined, 91
droppers, defined, 91
elevation of privileges, 90
environmental threats
defined, 89
local environment security, 607–608, 612–614
event frequency, estimating, 118–119
exploit kits, defined, 91
exploits, defined, 91, 566
flooders, defined, 91
hackers (crackers), defined, 92
hostile actors, 89
human-caused physical threats, local environment security, 609, 615
ICS, 228–229
identifying, 89
information disclosure, 90
injection flaws, defined, 92
intelligence, 563
analyzing threats, 569–570
benefits of, 566–568
gathering, 568–569
importance of, 566–568
SIEM, defined, 569
sources of threats, 564
types of threats, 564–565
keyloggers, defined, 91
local environment security
environmental threats, 607–608, 612–614
human-caused physical threats, 609, 615
technical threats, 608–609, 614–615
logic bombs, defined, 90
malware, defined, 90
mobile codes, defined, 91
mobile devices, 236–237
office equipment, 217
DoS attacks, 218–219
information disclosure, 218
network services, 217–218
password attacks, defined, 92
phishing, defined, 92
physical security
environmental threats, 607–608, 612–614
human-caused physical threats, 609, 615
technical threats, 608–609, 614–615
privacy threats, 189–191
ransomware, defined, 90
remote access attacks, defined, 92
repudiation threats, 89
risk assessment, determining future problems, 79
rootkits, defined, 91
social engineering, defined, 92
sources of, 564
spam, defined, 90
spammer programs, defined, 91
spoofing identity, 89
spyware, defined, 91

https://t.me/learningnets

STRIDE threat model, 89–90
technical threats, local environment security, 608–609, 614–615
Trojan horses, defined, 91
types of, 564–565
virus generators (kits), defined, 91
viruses, defined, 90
website exploits, defined, 92
worms, defined, 90
zero-day threats, defined, 567
zombies (bots), defined, 91
TIA-492, 423–426
tiny fragment attacks, 411
traffic analysis/eavesdropping, wireless network security, 427
training, role-based training, security awareness/education, 173–174
trapdoors (backdoors), 91, 488
Trojan horses, 91, 489
true negatives (intrusion detection), 505
true positives (intrusion detection), 505
trust relationships, 369
Trustwave Global Security Reports, 97
truth, single version of. *See* golden records

U

U.S. privacy laws/regulations, 195
UAT (User Acceptance Testing), 251
undervoltage (power outages), 608
UNIX, password schemes, 315–316
user authentication, 304, 307
authenticators, 311
biometric authentication, 330–331
AAL, 341–347
accuracy of, 333, 335–336
artifact detection, 340
biometric spoofing, 339
costs of, 333
cryptographic devices, 345
FMR, 335–336
FNMR, 335–336
liveness detection, 340
lookup secrets, 345
memorized secrets, 345
operating characteristic curves, 336
operation of, 333–335
OTP devices, 345
PAD, 339–340
physical characteristics used in, 332–333
presentation attacks, 339–340
risk assessment, 341–347
security controls, 339–341
SP 800-63B guidelines, 340–341
threats to, 337–339
cryptography and, 518
factors of, 310–311
hardware tokens, 322, 325–327
memory cards, 322–323
OTP devices, 328–329
security controls, 330
smart cards, 323–325
threats to, 329–330
inherence factor, 310
knowledge factor, 310
multifactor authentication, 311–312
NIST SP 800-63 Digital Identity Model, 307–310
passwords. *See* passwords
possession factor, 310
VoIP networks, 443
users
mistakes, exploiting, 314
passwords, 320
testing, defined, 265
user needs versus security implementation, 6

V

vacations, human resource security, 165
value proposition, 123
Verizon, Data Breach Investigations Reports, 93–94, 294
vetting applications, 240–241
virtual patching, ModSecurity WAF, 293

https://t.me/learningnets

virtualization. *See also* servers
container virtualization, 85, 374
hosted (nested) virtualization, 372, 377
hypervisors, 371
functions of, 371
security, 376
types of, 371–374
infrastructure security, 376
native virtualization, 371–372, 373
NFV, 85
security
hosted virtualization security, 377
hypervisors, 376
infrastructure security, 376
issues with, 374–375
VM, 370, 371
virus generators (kits), 91, 488
viruses, 489
antivirus software, cyber attack kill chains, 574
defined, 90
real-time antivirus software, VoIP networks, 443
VM (Virtual Machines), 370
defined, 84
guest OS, 371
VoIP (Voice over Internet Protocol) networks, 438
context, 440–442
processing, 439–440
security, 443
signaling, 439
threats, 442–443
VPN (Virtual Private Networks), 417–418
defined, 241
external network connections, 428
firewall-based VPN, 420
VoIP networks, 443
wireless network security, 426–427
vulnerabilities, 547
categories of, 103
CERT teams, 548
controls, 101
defined, 5, 76
determining risk, 78
discovering known vulnerabilities, 548–549
estimating, 119–120
ICS, 228–229
identifying, 102
ISC, 549
logs/reports, 551
mobile devices, 236–237
NVD, 103–104
CVSS metrics, 105–107
scoring example, 104–105
office equipment, 217
DoS attacks, 218–219
information disclosure, 218
network services, 217–218
Packet Storm, 549
patch management, 551–554
planning, 547–548
remediating vulnerabilities, 551–554
risk assessment, determining future problems, 80
scanning for vulnerabilities, 549–551
SecurityFocus, 549

W

WAF (Web Application Firewalls), 291–293, 574
WAP (Wireless Access Points)
network management, 416
SSID, 426
warm site backups, 386
waterfall development, 249
web analytics, 573
web applications
Open Web Application Security Project, 290–291
security, 293
policies, 294–295
risks, 289–291
WAF, 291–293
web drive-bys, 489

https://t.me/learningnets

web server logs, 557
websites, exploits, 92
whitelisting
application whitelisting, 164, 229
defined, 164
wireless networks
managing, 416–417
security
hackers (crackers), 427
network management, 426–427
VPN, 426–427
WAP, SSID, 426
WMI (Windows Management Instrumentation), 576
work flows (organizational information/ decision), cybersecurity management process, 36–37
workstation hijacking, 313
worms, 90, 489

X - Y - Z

X.816 security audit and alarms framework. *See* security monitoring, security audits
X.1055 risk management process, 80–81
zero-day threats, 567
zombies (bots), 91, 489

https://t.me/learningnets



VIDEO TRAINING FOR THE **IT PROFESSIONAL**

LEARN QUICKLY
Learn a new technology in just hours. Video training can teach more in less time, and material is generally easier to absorb and remember.

WATCH AND LEARN
Instructors demonstrate concepts so you see technology in action.

TEST YOURSELF
Our Complete Video Courses offer self-assessment quizzes throughout.

CONVENIENT
Most videos are streaming with an option to download lessons for offline viewing.

Learn more, browse our store, and watch free, sample lessons at
informit.com/video

Save 50%* off the list price of video courses with discount code **VIDBOB**

Pearson

informIT®
the trusted technology learning source

*Discount code VIDBOB confers a 50% discount off the list price of eligible titles purchased on informit.com. Eligible titles include most full-course video titles. Book + eBook bundles, book/eBook + video bundles, individual video lessons, Rough Cuts, Safari Books Online, non-discountable titles, titles on promotion with our retail partners, and any title featured as new on the Pearson IT Certification store are not eligible for discount. Discount may not be combined with any other offer and is not redeemable for cash. Offer subject to change.

https://t.me/learningnets



REGISTER YOUR PRODUCT at informit.com/register

Access Additional Benefits and SAVE 35% on Your Next Purchase

- Download available product updates.
- Access bonus material when applicable.
- Receive exclusive offers on new editions and related products. (Just check the box to hear from us when setting up your account.)
- Get a coupon for 35% for your next purchase, valid for 30 days. Your code will be available in your InformIT cart. (You will also find it in the Manage Codes section of your account page.)

Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.

InformIT.com–The Trusted Technology Learning Source

InformIT is the online home of information technology brands at Pearson, the world's foremost education company. At InformIT.com you can

- Shop our books, eBooks, software, and video training.
- Take advantage of our special offers and promotions (informit.com/promotions).
- Sign up for special offers and content newsletters (informit.com/newsletters).
- Read free articles and blogs by information technology experts.
- Access thousands of free chapters and video lessons.

Connect with InformIT–Visit informit.com/community

Learn about InformIT community events and programs.

informIT.com
the trusted technology learning source

Addison-Wesley • Cisco Press • IBM Press • Microsoft Press • Pearson IT Certification • Prentice Hall • Que • Sams • VMware Press

ALWAYS LEARNING
https://t.me/learningnets
PEARSON

Appendix C

Answers to Review Questions

Chapter 1

1. The following terms are defined from a cybersecurity perspective:

   - **Availability—**The property of a system or a system resource being accessible, or usable, or operational upon demand by an authorized system entity, according to performance specifications for the system. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, and maintaining a correctly functioning operating system environment that is free of software conflicts.
   - **Integrity—**This means maintenance of consistency, accuracy, and trustworthiness of data over its entire life cycle. There should not be any change in data in transit, such as unauthorized people altering data (for example, in a breach of confidentiality). These measures include encryption, file permissions, and user access controls.
   - **Authenticity—**This is simply the property of being genuine and being able to be verified and trusted. It is a technological concept and can be solved by cryptography. Authenticity is about one party, Alice, interacting with another, Bob to convince Bob that some data really comes from Alice.
   - **Non-repudiation—**This is a legal assurance that the sender of information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. For example, non-repudiation is about Alice showing to Bob a proof that some data really comes from Alice, such that not only is Bob convinced, but Bob also gets the assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob
   - **Confidentiality—**This, in lay terms, is privacy. It is a set of rules that limits access to information from reaching the wrong people, while making sure that the right people can

https://t.me/learningnets

in fact get it. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs, or soft tokens.

2. Three key challenges in developing an effective cybersecurity system are as follows:
   - **Scale and complexity of cyberspace—**Many telecom companies, such as Ericsson, are working to connect all devices and people to each other to make a fully connected society by next decade. It would cut across wired, wireless, and satellite networks and would consist of mobile devices, PDAs, laptops, wearables, cars, Internet of Things (IOT) devices, the cloud, and so on. The challenges to achieving cybersecurity will change with each technological advancement because new applications of information technology will emerge, which will trigger massive changes in societal norms.
   - **Nature of threat—**It will come from both internal sources and external sources. Common actors involved are vandals, criminals, terrorists, hostile states, and other malevolent actors. The desire to collect, analyze, and store individual information by both government agencies and corporations will create security and privacy risks.
   - **Trade-off between user needs and security implementation—**It is a heavily debated topic that involves huge trade-offs because users wants to use the most recent technology without caring for overall security, whereas an enterprise wants security and continuity at all costs. For example, employees prefer to connect their personal devices to the office network and share content, but this might introduce potent viruses and malware that could infect the whole system in a short time.
3. Big organizations employ a mix of many technologies, such as cryptography, network security protocols, operating system mechanisms, database security schemes, firewall, and antivirus protection.
4. The most significant activity of the ISF is the ongoing development of the Standard of Good Practice for Information Security (SGP). This document is a focused reference guide for enterprises to identify and manage information security risks in their operations and supply chains. This document is well researched, with input from its members, as well as an analysis of the leading standards on cybersecurity, information security, and risk management.
5. The three key activities for information security, according to the SGP, are as follows:
   - Planning for cybersecurity
   - Managing the cybersecurity
   - Assessment of security
6. An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. An ISMS is primarily implemented to

https://t.me/learningnets

minimize all types of risk and ensure business continuity by proactively limiting the impact of a security breach. An ISMS typically addresses employee behavior and processes as well as data and technology. ISO 27001 is the default standard for establishing and maintaining ISMSs in enterprises.

7. Five core functions mentioned in the NIST framework are as follows:
   - **Identification—**This implies development of organizational understanding of management of cybersecurity risk to systems, assets, data, and capabilities.
   - **Protection—**This implies development and implementation of appropriate safeguards for ensuring delivery of critical infrastructure services.
   - **Detection—**This implies development and implementation of appropriate activities for identification of any occurrence of a cybersecurity event.
   - **Response—**This implies development and implementation of appropriate activities for taking action regarding a detected cybersecurity event.
   - **Recovery—**This implies development and the appropriation of activities needed for maintenance of plans for resilience and for restoration of capabilities or services impaired due to a cybersecurity event.
8. The weakest link in an information security chain is the people employed by or associated with the organization.

Chapter 2

1. Both terms have their own scope and definition. *Security governance* is the system by which an organization directs and controls its overall security, thereby meeting all strategic needs of the organization. *Security management* is concerned with making decisions to mitigate risks by using the information as input and then applying it in the risk management process.

   Governance determines decision-making authority. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies, whereas governance ensures that these security strategies are aligned with business objectives and consistent with regulations.
2. The three supplemental factors—internal incident and global vulnerability reports, standards and best practices, and user feedback—are all part of the success of any security management system. Internal security incident reports and global vulnerability reports from various sources illuminate possible security breaches/violations that help define the threat and the level of risk that the organization faces in protecting its information assets. The numerous standards and best practices documents provide guidance on managing risk. User feedback (both internal and external) helps improve the effectiveness of policies, procedures, and technical mechanisms.

https://t.me/learningnets

3. Primary, or *internal*, stakeholders are parties (either individuals or groups) that actively run the management of the company. They can influence and can be influenced by the success or failure of the entity because they have a vested interest in the organization. Some examples of internal stakeholders of an organization are employees, owners, members of the board of directors, managers, and investors. Secondary, or *external*, stakeholders are interested parties who are not a part of the management but who indirectly affect the company's working and in turn are affected by the outcome. They are the outside parties that form part of the business operation chain. Some examples of external stakeholders of a company are customers, suppliers, creditors, third-party contractors, competitors, society, and government.
4. The two key pillars on which IT strategy planning should be based are mission necessity and enterprise maturity.
5. The three categories of metrics for evaluating an organization's security governance are as follows:
    - **Executive management support—**This is the most critical component for the success of any cybersecurity program. In order for the effect to perpetuate to lower layers, top executives must exhibit an understanding of security issues and take a proactive role in promoting security.
    - **Business and information security relationship—**There has to be a strong and symbiotic relationship between business goals and objectives and information security in any organization. When information security is incorporated into the enterprise planning process, employees feel empowered to secure their assets and view security not as an impediment but as an enabler of success.
    - **Information protection—**This is concerned with the pervasiveness and strength of information security mechanisms. These indicators reflect the degree of awareness of information security issues and the level of enterprisewide preparedness to deal with actual attacks.
6. COBIT 5 enumerates five distinct roles or structures for the security governance body:
    - **Chief information security officer (CISO)—**The CISO carries overall responsibility for the enterprise information security program. The CISO acts as a bridge between executive management and the information security program and effectively communicates and coordinates closely with key business stakeholders to address information protection needs.
    - **Information security steering (ISS) committee—**This committee ensures constant monitoring and review to ensure that good practices in information security are applied effectively and consistently throughout the enterprise. It acts as a watchdog.
    - **Information security manager (ISM)—**The ISM holds overall responsibility for the management of all aspects of information security.

https://t.me/learningnets

- **Enterprise risk management (ERM) committee—**This is the main decision-making body of the enterprise to assess, control, optimize, finance, and monitor risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.
- **Information custodians/business owners—**They act as intermediaries between the business and information security functions.

7. The acronym RACI stands for *responsible, accountable, consulted, and informed*. It is used in the form of a matrix that explains the levels of responsibilities of all stakeholders in each of the key activities of the work:

   - **Responsible—**The person/group/team that performs the activity and is expected to deliver/submit the assigned work portion within the given deadline. For example, in an office transport system, the driver is responsible.
   - **Accountable—**The person /group/team that has decision-making authority and is expected to ensure the successful completion of the activity. For example, in an office transport system, the manager of the team of drivers is accountable.
   - **Consulted—**The person /group/team that should be included in the decision-making process for the activity because this person's/group's/team's responsibilities cover the outcome of this activity. For example, in an office transport system, the administrative head of the office should be consulted.
   - **Informed—**The person /group/team that needs to know of a decision or an action after it occurs in order to plan things based on the outcome. For example, in an office transport system, the manager of the employees who are using the office transport should be informed.

Chapter 3

1. Fair and accurate risk assessment enables an organization to determine an appropriate budget for security and implement appropriate security controls that optimize the level of protection while not overshooting the budget. Risk assessment enumerates potential security breaches, fair estimates of their cost, and the likelihood of their occurrence. Without risk assessment, an organization cannot formulate a cost-effective strategy to secure itself.
2. Residual risk is the remaining portion of a threat after all efforts to identify and eliminate risk have been made. In other words, residual risk is the output of risk treatment applied on a potential threat. For example, an athlete can transfer residual risk by insuring his body parts.
3. A threat is a capability of a threat source to intentionally or accidentally trigger vulnerability in the system. A vulnerability is a weakness or potential and intentional entry point in a system. Vulnerabilities can be in security procedures, design, implementation, or internal controls. A threat that cashes in on a potent vulnerability will produce a security violation, or breach.

https://t.me/learningnets

4. The four contributing factors to determine risk in any organization are as follows:
   - **Asset—**Anything that can be a given a monetary value is an asset of an organization. Valuation of an asset is crucial to determine the impact of a risk and its subsequent treatment.
   - **Threat—**Any risk that has a potential to damage an asset is a threat. For any threat, past history is a good indicator of its frequency and possible impact.
   - **Vulnerability—**Any trapdoor or unintended weak point of a system is as vulnerability. A threat can ride on a potential vulnerability and damage a system if not stopped early.
   - **Control—**A control is an action to stop a potential threat from causing damage. A control is specific to the threat and thus needs to be chosen judiciously because this choice has major impacts on cost, functionality, and continuity of the system.
5. A qualitative risk assessment prioritizes the identified risks using a predefined rating scale (1 to 10, 1 to 7, and so on). Risks are scored based on their probability or likelihood of occurring (0 to 1) and the impact on project objectives should they occur. This is grossly subjective and is based on past history, heuristics, and expert judgment. A quantitative risk assessment is a purely mathematical approach to prioritizing risks by calculating/deriving a numerical or quantitative rating for each risk and then summing up and normalizing to arriving at overall risk.
6. Key ingredients of a sample risk analysis worksheet are as follows:
   - **Security issues—**This gives a brief statement of the security issue or area of concern as well as a description of compliance issues.
   - **Likelihood—**This is estimated (by internal experts or using past history or heuristics) likelihood for an occurrence of the linked threat/vulnerability pair.
   - **Impact—**This is the estimated impact (financial/temporal/spatial) for the linked threat/vulnerability pair.
   - **Risk level—**This is assessed according to the matrix shown in Figure 3.8 of Chapter 3.
   - **Recommended security controls—**These are specific security controls recommended by the team.
   - **Control priorities—**These are the relative priorities of the recommended controls.
   - **Comments—**This is a relevant note for the security risk management decision-making process linked with this security issue.
7. The six stages of information security risk management process are described as follows:
   - **Context establishment—**Here you set the basic criteria necessary for information security risk management, define the scope and boundaries, and establish an appropriate organization operating the information security risk management.

https://t.me/learningnets

- **Risk assessment—**Here you identify the risk to analyze it thoroughly and then to evaluate the risk against establish metrics to categorize it for further action.
- **Risk treatment—**Here you mitigate risk by either stopping/removing the source of risk or change its probability of happening or change its possible impact or hedge the risk with a third party or transfer the risk by outsourcing or living with the risk.
- **Risk acceptance—**The risk post-treatment process should be explicitly communicated to managers/decision makers with the caveat that it cannot be reduced further and should be accepted.
- **Risk communication and consultation—**This is the continual and iterative processes an organization follows to provide, share, or obtain information about the risk and to keep updating or taking feedback from the key stakeholders regarding the management of risk.
- **Risk monitoring and review—**This stage involve continuous monitoring and review of all risk information obtained from the risk management activities.

8. The four risk-related standard documents that are published by Open Group are as follows:
   - The Open Group Standard: Risk Taxonomy (2013)
   - The Open Group Technical Guide : Requirements for Risk Assessment Methodologies (2009)
   - The Open Group Technical Guide: FAIR—ISO/IEC 27005 Cookbook (2010)
   - The Open Group Risk Analysis (O-RA) Technical Standard (2013)
9. FAIR defines the key terms as follows:
   - **Asset—**Any data, device, or other component of the environment that involves information and that can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss
   - **Risk—**The probable frequency and probable impact of future loss
   - **Threat—**Any entity capable of harming an asset and/or organization partially or permanently
   - **Vulnerability—**The probability of an asset's inability to resist actions of a threat agent

   FAIR definitions are much more specific than ISO 27005 definitions pertaining to risk analysis.
10. Regarding risk assessment, you consider the following types of assets:
    - **Hardware assets—**This includes physical servers, workstations, laptops, mobile devices, removable media, PDA devices, television sets, and networking and telecommunications equipment.

https://t.me/learningnets

- **Software assets—**This includes applications, operating systems and other system software, virtual machine and container virtualization software, software for software-defined networks (SDNs) and network function virtualization (NFV), database management systems (DBMSs), decision support systems (DSS), and analytic engine (AEs).
- **Information assets—**This includes assets directly connected with information or its storage (for example, databases, file systems, cloud storage, routing information). This category of asset depends on the nature of work done by the organization.
- **Business assets—**This category includes all other organization assets (such as human capital, business processes, and factory location) that don't fit in preceding categories of assets. It also includes intangible assets, such as organization control, know-how, reputation, and image of the organization.

11. STRIDE is a threat classification system developed by Microsoft to categorize deliberately planned attacks. It includes identity spoofing, data tampering, repudiation, information disclosure to non-authorized entities, denial-of-service (DoS), privilege elevation, and so on. For example, imagine that a bright engineering team of company X is working on a new high-end mobile phone. The product is announced, and the CEO of X describes it capabilities and fixes its release date. All is going fine until a key member of the design team voluntarily discloses design specifications (for extra money and a better job than his current one) and implementation-level details to the company's key competitor, say Y. As a result, Y improves the specifications, adds more capability, and, following an Agile go-to-market strategy, it announces an earlier release date. This results in X's image being downgraded, its share price crashing, investors losing confidence, and a complete panic in the design team. This is a classic case of involuntary information disclosure.
12. Some common cybersecurity threat forms are malware, virus, worm, ransomware, spam, Trojan horse, trapdoor, exploits, spam programs, flooders, zombies/bots, spyware, adware, DNS attacks, DoS attacks, remote access attacks, phishing, sniffing, website exploit, and password attack.
13. The three key themes in the Threat Horizon report are as follows:
    - **Disruption—**This can be caused by overreliance on existing connectivity and planning processes of doing business.
    - **Distortion—**Once information integrity is lost, the monitoring of access and changes to sensitive information will become critical. This also leads to development of complex incident management procedures.
    - **Deterioration—**This occurs when controls are dictated by regulations and technology bringing a heightened focus on risk assessment and management in light of regulatory changes and the increased prevalence of artificial intelligence in everyday technology.

https://t.me/learningnets

14. The FAIR risk analysis document groups controls into four categories:

    - **Avoidance controls—**This type of control affects the frequency and/or likelihood of threats encountered. These controls include firewall filters, physical barriers, and relocation of assets and reduction of threat populations.
    - **Deterrent controls—**This type of control affects the likelihood of a threat causing possible damage. These controls include policies, logging and monitoring, and enforcement practices.
    - **Vulnerability controls—**This type of control affects the probability that a threat's action will result in loss. These controls include authentication, access privileges, and patching.
    - **Responsive controls—**This type of control affects the amount of loss that results from a threat's action (that is, loss magnitude). These controls include backup and restore media and processes, forensics capabilities, and incident response processes.

15. ISO 27005 lists four options for treating risk:

    - **Risk reduction or mitigation—**This implies actions taken to lessen the probability and/or negative consequences associated with a risk.
    - **Risk retention—**This implies acceptance of the cost from a risk.
    - **Risk avoidance—**This implies a decision not to become involved in or an action to withdraw from a risk situation.
    - **Risk transfer or sharing—**This implies sharing the burden of loss from a risk with a third party, such as an insurance agency.

16. Three elements define the scope of risk assessment:

    - **Services—**This includes business services, such as sales and marketing, business processes, such as inventory management, and technical services, such as configuration management.
    - **Assets—**This includes human capital, information, physical devices, software, and physical plant assets.
    - **Factors influencing impact ratings—**This includes economic, social, technological, legal, and environmental factors.

Chapter 4

1. The security management function encompasses establishing, implementing, and monitoring and information security program, under the direction of a senior responsible person or specialized team. The organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements.

https://t.me/learningnets

2. The two key individual roles in security management are as follows:

   - **Chief information security officer (CISO)—**This person holds overall responsibility for the enterprise information security program in the organization. The CISO links executive management with the information security program. The CISO should also communicate and coordinate closely with key business stakeholders to address information protection needs.
   - **Information security manager (ISM)—**This person holds overall responsibility for the management of information security efforts, including application information security, infrastructure information security, access management, threat and incident management, risk management, awareness program, metrics, and vendor assessments.

3. Key security program areas are as follows:

   - **Security planning—**Security planning primarily includes the alignment of information security management and operations with enterprise and IT strategic planning. It also includes more detailed planning for the organization, coordination, and implementation of security.
   - **Capital planning—**Capital planning is meant to facilitate and control the expenditure of the organization's funds. Its main aim is to prioritize potential IT security investments for allocating available funding to maximize profit.
   - **Awareness and training—**Awareness and training programs ensure that all employees of the organization understand their information security responsibilities to properly use and protect the information resources entrusted to them.
   - **Information security governance—**The CISO along with other C-level executives (CEO, CFO, CTO, and so on) and the board develop an effective security governance charter.
   - **System development life cycle—**This is about the development, implementation, and replacement of information systems.
   - **Security products and services acquisition management—**This is about supervision of the acquisition of security-related products and services, including considering the costs involved, the underlying security requirements, and the impact on the organizational mission, operations, strategic functions, personnel, and service provider arrangements.
   - **Risk management—**This is the prediction and evaluation (mostly financial) of risks together with the identification of procedures to avoid or minimize their impact on the organization.
   - **Configuration management—**This implies adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

https://t.me/learningnets

- **Incident response—**Incident response occurs after the reporting of a security event. It aims to minimize the damage of the event and facilitate rapid recovery.
- **Contingency planning—**Information system contingency planning refers to management policies and procedures designed to maintain or restore business operations, including computer operations (possibly at an alternate location) in the event of emergencies, system failures, or disasters.
- **Performance measures—**Performance measures, a key feedback mechanism for an effective information security program, should be defined and used across the entire organization.

4. The Select/Control/Evaluate framework defines a cyclical process consisting of three steps for deciding which projects to pursue or which investments to make:
   - **Select phase—**Here the organization identifies and analyzes each project's risks and returns to determine financial feasibility before committing significant funds to any project. The organization then selects IT projects that will align best with its future plans. This process should be repeated each time funds are allocated to projects.
   - **Control phase—**Here the organization ensures that, as a project progresses, it continues to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps must be quickly taken to address the deficiencies. If the mission needs have changed, the organization needs to adjust its objectives for the project and appropriately modify expected project outcomes.
   - **Evaluate phase—**Here a comparison is done between actual and expected results after project completion.
5. An information security policy is framed to ensure that all employees in an organization, especially those with responsibility of some sort for one or more assets, understand the security principles in use and their individual security-related responsibilities. Ambiguity in information security policies can defeat the purpose of the security program and may result in significant losses in all aspects. An information security policy is the central tool of an organization to provide management direction and support for information security across the organization. The security policy document defines the ideal expectations and proper behavior for employees, contractors, vendors, and all others who have roles in the organization.

   Some of the documents related to security are the information security plan, strategic plan, security plan, security policy, and acceptable use policy.
6. Some common security policies of an organization are as follows:
   - Access control policy
   - Contingency planning policy
   - Data classification policy

https://t.me/learningnets

- Change control policy
- Wireless policy
- Incident response policy
- Termination of access policy
- Backup policy
- Virus policy
- Retention policy
- Physical access policy
- Security awareness policy
- Audit trail policy
- Firewall policy
- Network security policy
- Encryption policy

7. A prototypical structure of a security document should contain following items:
   - **Overview—**Background information about the issue the policy addresses.
   - **Purpose—**Why the policy is being created.
   - **Scope—**What areas the policy covers.
   - **Targeted audience—**To whom the policy is applicable.
   - **Policy—**A complete but concise description of the policy.
   - **Noncompliance—**Consequences for violating the policy
   - **Definitions—**Technical terms used in the document.
   - **Version—**The version number to control the changes made to the document.
8. The key aspects of a security policy document are as follows:
   1. **Responsibilities—**This aspect identifies:
      - Those responsible for ratifying policy document (for example, the board)
      - Responsibilities of all relevant individuals to comply with the policy
      - Individuals responsible for protecting specific assets
      - That all individuals must confirm the understanding of, acceptance of, and compliance with relevant policies and understand that disciplinary action will follow policy violation

https://t.me/learningnets

2. **Principles—**This aspect specifies the following:
   - All relevant assets to be identified and classified by value/importance
   - All assets protected with respect to CIA (confidentiality, integrity, and availability) and other security requirements
   - All laws, regulations, and standards are complied with
3. **Actions—**This aspect specifies the following:
   - That all individuals are made aware of the security policy and their responsibilities
   - That all assets are subject to risk assessment periodically and before a major change
   - That all breaches are reported in a systematic fashion
   - That auditing occurs periodically and as needed
   - That policy documents are reviewed regularly and as needed
4. **Acceptable use—**This aspect specifically documents the following:
   - What behaviors are required, acceptable, and prohibited with respect various assets
   - Responsibility for establishing, approving, and monitoring acceptable use policies

9. Information security management performs the following functions:
   - **Consistent organizationwide use of security—**The CISO or other responsible authority should develop, maintain, and regularly review an overall security strategy for the organization and the accompanying policy document.
   - **Support function—**The CISO or other responsible authority should act as a security adviser and a security evangelist in the organization and oversee security aspects in all documents across the organization.
   - **Monitor function—**The CISO or other responsible authority should monitor trends and developments to be aware of how they may affect the organization's security strategy and implementation, including in the area of business trends, new technical developments, security solutions, standards, legislation, and regulation.
   - **Projects function—**The CISO or other responsible authority should be responsible for overseeing security-related projects.
   - **External requirements function—**The CISO or other responsible authority should manage the implications of laws, regulations, and contracts.
10. An acceptable use policy (AUP) is a type of security policy targeted at all employees who have access to one or more organization assets. It defines what behaviors are acceptable and what behaviors are not acceptable. The policy should be clear and concise, and it should be a condition of employment for each employee to sign a form indicating that he or she has read and understood the policy and agrees to abide by its conditions.

https://t.me/learningnets

Chapter 5

1. The employment life cycle is a human resources model that identifies stages in employees' careers to help guide their management and optimize the company's performance. It is a relationship of the individual to the organization prior to employment, during employment, and post-employment (resignation/termination). One way to define the employment life cycle is to see it as having five stages:
    1. Recruitment
    2. Onboarding
    3. Career planning
    4. Career development
    5. Termination/resignation
2. You can categorize the security problems caused by employees into two divisions:
    - **Unintentional and originating from carelessness—**Some employees, unknowingly or out of sheer carelessness, aid in the commission of security incidents by failing to follow proper procedure, by forgetting security considerations, and by not understanding what results their actions can have. These people have no motive to cause harm. It may be either accidental, when there is no decision to act inappropriately, or it may be negligent, when there is a conscious decision to act inappropriately. In the latter case, someone may take a shortcut to increase productivity or simply to avoid hassle but feels he or she can do so without causing a security incident.
    - **Malicious intent and deliberate—**A minority chunk of employees knowingly violates all controls and procedures to causes or aids in an incident. The security problems caused by such persons can exceed those caused by outsiders, as employees with privileged access are the ones who know the controls and who know what information of value may be present. These incidents are hard to track.
3. General guidelines for checking applicants are as follows:
    - Ask for as much detail as possible about employment and educational history. The more detail that is available, the more difficult it is for the applicant to lie consistently. Check this data with online tools such as LinkedIn to verify authenticity.
    - Investigate the accuracy of the details (using a background or criminal check) to the extent reasonable by outsourcing it to some verification agency.
    - Arrange for experienced staff members to interview candidates face-to-face and try to gauge each candidate's expectations and fit with the proposed profile and company.

https://t.me/learningnets

- Check the applicant's credit record for evidence of large personal debt and inability to pay it.
- Ask the applicant to obtain bonding for his or her position if the company expects to spend a significant amount in hiring/training this person or sending him or her abroad on a work visa to work on its behalf.

4. Any company can ensure personnel security by following these principles:
   - **Least privilege—**Give each person the minimum access necessary to do his or her job. This restricted access is both logical (access to accounts, networks, programs) and physical (access to computers, backup tapes, and other peripherals). If every user has accounts on every system and has physical access to everything, then all users are roughly equivalent in their level of threat.
   - **Separation of duties—**Carefully separate duties so that people involved in checking for inappropriate use are not also capable of perpetrating such inappropriate use. Having all the security functions and audit responsibilities entrusted to the same person is dangerous. This practice can lead to a case in which the person may violate security policy and commit prohibited acts, yet no other person sees the audit trail or is alerted to the problem.
   - **Limited reliance on key employees—**No one in an organization is irreplaceable. If your organization depends on the ongoing performance of a key employee, then your organization is at risk. Organizations cannot help but have key employees. To be secure, organizations should have written policies and plans established for unexpected illness or departure. As with systems, redundancy should be built into the employee structure. There should be no single employee with unique knowledge or skills.
5. The security officer of Alpha should take the following actions before relieving X from services of Alpha:
   1. Remove X's name from all lists of authorized access.
   2. Explicitly inform guards that X is not allowed into the building without special authorization by named employees.
   3. Take away any car parking sticker, official drawer/cupboard, and so on from X.
   4. If appropriate, change lock combinations, reprogram access card systems, and replace physical locks.
   5. Remove all personal access codes.
   6. Recover all assets, including employee ID card, disks, documents, and equipment.
   7. Check whether all relevant stakeholders have given no objection to Mr. X's termination.
   8. Notify, by memo or email, appropriate departments so that they are aware of the change in employment status.

https://t.me/learningnets

6. The four levels of the cybersecurity learning continuum are as follows:
   - **Awareness—**A set of activities that explains and promotes security, establishes accountability, and informs the workforce of security news. Participation in security awareness programs is required for all employees.
   - **Cybersecurity essentials—**Intended to develop secure practices in the use of IT resources. This level is needed for those employees, including contractor employees, who are involved in any way with IT systems. It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.
   - **Role-based training—**Intended to provide knowledge and skills specific to an individual's roles and responsibilities relative to information systems. Training supports competency development and helps personnel understand and learn how to perform their security roles.
   - **Education/certification—**Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social).
7. The goals for a security awareness program should include the following:
   - Provide a focused approach for all awareness, training, and educational activities related to information security, with better coordination to make it more effective.
   - Communicate key recommended guidelines or practices required to secure information resources.
   - Provide general and specific information about information security risks and controls to people on a need basis.
   - Make individuals aware of their responsibilities in terms of information security.
   - Motivate individuals to adopt recommended guidelines or practices by giving incentives (corporate goodies).
   - Create a stronger culture of security with individual commitment to information security.
   - Help enhance the consistency and effectiveness of existing information security controls and potentially stimulate the adoption of cost-effective controls.
   - Help minimize the number and extent of information security breaches, thus reducing costs directly (for example, data damaged by viruses) and indirectly (for example, reduced need to investigate and resolve breaches).
8. Impart awareness training by using the following instruments:
   - Brochures, leaflets, and fact sheets
   - Security handbook

https://t.me/learningnets

- Regular email or newsletter
- Distance-learning web courses
- Workshops and training sessions by both internal and external sources
- Formal classroom coaching
- Online video tutorials
- A separate security website
- Email advisories issued by industry-hosted news groups, academic institutions, or the organization's IT security office
- Professional organizations and vendors
- Online IT security daily news websites
- Periodicals
- Conferences, seminars, and workshops

9. Bring your own device (BYOD) is a strategy adopted by an organization that allows employees, business partners, and other users to utilize a personally selected and purchased client device to execute enterprise applications and access company data. A BYOD policy usually spans personal laptops, smartphones, and tablets. It can have various options, depending on the level of access and type of devices. Some challenges in implementing a BYOD strategy are as follows:

    - **Data management issues—**With mobile and cloud data storage solutions, it has become difficult to manage and track data, especially when devices have seamless connectivity and huge storage. It is not easy to distinguish between work data and personal data, and often companies have use third-party solutions to monitor data movement.
    - **Data compliance issues—**With the increased incidence of identity theft and phishing scams everywhere, government authorities have come up with strict regulations for data management. These measures increase operation and capital cost of doing business, and BYOD policies increase the complexity.
    - **Malicious applications—**Personal devices are vulnerable to malware and malicious apps. Further, an organization needs to be concerned about unauthorized access to corporate data via mobile apps. When employees download malicious apps on their cellphones, they give outsiders unauthorized access to critical corporate data. It is a headache to impose security software and add updates and patches on these devices.
    - **Lost or stolen devices—**Whenever devices that are registered in a BYOD network are lost or stolen, there is a high probability that sensitive corporate data can fall into the hands of an outsider with malicious intent.

https://t.me/learningnets

- **Fired/disgruntled outgoing employees—**Employees can easily retain a certain amount of data (by making backups) even after they leave an organization. It is impractical for the HR department to check the data residing on an employee's smartphone, and such information can easily be leaked to a rival organization.
- **Hacking issues—**These days, it is easy to hack mobile devices. When a device is hacked, it can be used to connect to a corporate network to access business-critical information.

10. An ideal cybersecurity program should include following points:
    - Technical points about cybersecurity and its taxonomy, terminology, and challenges, with subtle details
    - Common information and computer system security vulnerabilities
    - Common cyber attack mechanisms, their consequences, and motivations behind them
    - Different types of cryptographic algorithms
    - Intrusion, types of intruders, techniques, and motivation
    - Firewalls and other means of intrusion prevention
    - Vulnerabilities unique to virtual computing environments
    - Social engineering and its implications to cybersecurity
    - Fundamental security design principles and their role in limiting points of vulnerability
11. The following measures are suggested:
    - The organization should have documented procedures in place for protecting physical assets, such as mobile devices, USB drives, and documents. Further, the organization should have in place more stringent procedures for remote access to company servers and databases, as well as cloud services used by the company.
    - There should be support for remote working by imparting adequate training (for example, how to perform backups and encrypt files) and adequate technical support as well as allowing use of secure tools such as VPN access to allow remote access. For sensitive documents, an additional layer of security must be implemented.
    - Additional controls and support, in terms of handling of information and sensitive data, should be provided for employees traveling to high-risk countries.
12. Malicious behavior involves deliberate and conscious attempts to harm an organization by acting inappropriately. Examples include sharing business files with a competitor, insider trading, and destroying project data to cause deliberate loss to the organization.

https://t.me/learningnets

Negligent behavior is non-intentional but ignorant or lazy action to act inappropriately. It is often devoid of any motive to cause harm. Examples include using unauthorized services or devices to save time, doing personal work during office hours, and downloading movies from unsafe sites using office network.

Accidental behavior is non-intentional and non-deliberate action to act inappropriately. Such actions are usually done on impulse. Examples include emailing sensitive information to unauthorized recipients, opening malicious email attachments, publishing personal information on publicly available servers, and talking about a confidential product launch with a colleague in a public place.

Chapter 6

1. ISF's SGP divides information management into these four topics:
   - **Information classification and handling—**This encompasses methods of classifying and protecting an organization's information assets.
   - **Privacy—**This is broadly concerned with threats, controls, and policies related to the privacy of personally identifiable information (PII).
   - **Document and records management—**This covers the protection and handling of the documents and records maintained by an organization.
   - **Sensitive physical information—**This consists of specific issues related to the security of information assets in physical form.
2. The NIST risk management framework enumerates six steps for managing overall risk:
   1. **Categorization—**Here you identify information that will be transmitted, processed, or stored by the system and define applicable levels of information categorization based on an impact analysis.
   2. **Selection—**Here you select an initial set of baseline security controls for the system, based on the security categorization, and you tailor and supplement the security control baseline as needed.
   3. **Implementation—**Here you implement security controls and document how the controls are used within the system and its environment of operation.
   4. **Assessment—**Here you assess the security controls by using appropriate assessment procedures and try to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
   5. **Authorize—**This is about formal authority by the system to operate or continue to operate based on the results of the security control assessment. This decision is based

https://t.me/learningnets

on a determination of the risk to organizational operations and assets resulting from the operation of the system and the decision that this risk is acceptable.

6. **Monitor—**Here you persistently monitor security controls to ensure that they are effective over time as changes occur in the system and the environment in which the system operates.

3. FIPS 199 provides the following generic format to define a security category:

   SC information type = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}

4. The four steps in the security categorization process given by NIST SP 800-60 are as follows:

   1. **Identify information types—**In this step, you identify the information types for classification, resulting in an information taxonomy or catalog of information types. The level of detail, or granularity, must be decided by consensus of security governance personnel. They may base their decision on factors such as the size of the organization, its range of activities, and the perceived overall level of risk.
   2. **Select provisional impact levels—**Here you assign security impact levels for the identified information types.
   3. **Review and adjust provisional impact levels—**Here you review the provisional impact levels, allowing a range of managers and information owners to contribute to the process. This results in fine-tuning of impact levels.
   4. **Assign system security category—**Finally, you run the security classification process to assign a security classification for each information type. If you follow SP 800-60, the overall classification of an information type corresponds to its assessed impact, which is the highest of the confidentiality, integrity, and availability impacts.

5. The following three organizational sources, as suggested by SP 800-60, define individual information types.

   - **Mission-based information—**This area encompasses types of information that relate specifically to the mission of the organization. For example, an organization in the healthcare field has information on what healthcare delivery services it provides, fee schedules, insurance arrangements, and policies for providing financial help to clients. A technology company has information about its research and development plans and goals, outside consulting arrangements, and long-range plans for new technology.
   - **Services delivery support functions—**These are types of information that support the operation of the organization and relate to specific services or products offered by the organization. For example, in the area of risk management and mitigation, information types include contingency planning, continuity of operations, and service recovery.
   - **Back office support functions—**These support activities enable the organization to operate effectively. SP 800-60 identifies five main groups of information types in this area: administrative management, financial management, human resource management, information management, and technology management.

https://t.me/learningnets

6. In the context of information, the term *privacy* usually refers to making valuable private information about an individual unavailable to parties who have no permission (from the legitimate owner) as well as no direct need for that information. Privacy interests attach to the gathering, control, protection, and use of information about individuals and then using it for their own gains. For example, call centers handling credit card accounts leaking credit card details of subscribers to a marketing company would be a blatant violation of privacy.

7. The two terms are related. *Information security* can protect *privacy*. For example, an intruder seeking ostensibly private information (such as personal e-mails or photographs, financial or medical records, phone calling records) may be stymied by good cybersecurity measures. Additionally, security measures can protect the integrity of PII and support the availability of PII. But certain measures taken to enhance cybersecurity can also violate privacy. For example, some proposals call for technical measures to block Internet traffic containing malware before it reaches its destination. But to identify malware-containing traffic, the content of all in-bound network traffic must be inspected. But inspection of traffic by any party other than its intended recipient is regarded by some as a violation of privacy, because most traffic will, in fact, be malware-free. Under many circumstances, inspection of traffic in this manner is also a violation of law.

   Both these terms are very closely related and have a deep symbiotic relationship. *Information security* provides protection for all types of information, in any form, so that the information's confidentiality, integrity, and availability are maintained. *Privacy* assures that personal information is collected, processed (used), protected, and destroyed legally and fairly as per prevailing law of land.

8. Some possible types of threats in the information collection process are as follows:

   - **Surveillance—**This is the watching, listening to, or recording of an individual's activities without his or her consent or knowledge. This can be problematic and a violation of the right to privacy.
   - **Interrogation—**This is the act of pressuring an individual to divulge information by application of force (physical or mental). For example, if certain fields in a form or in an online registration process are required in order to proceed, the individual is compelled, or at least pressured, to divulge information that he or she would prefer not to.

9. Privacy can be violated at the information processing stage in the following ways:

   - **Aggregation—**Aggregation of data about an individual in various databases allows anyone with access to the aggregated data to learn more about an individual than could be learned from separate, and separately protected, data sets.
   - **Identification—**It is possible, with sufficient data, to be able to aggregate data from various sources and use those data to identify persons who are not otherwise identified in the data sets.

https://t.me/learningnets

- **Insecurity—***Insecurity* refers to the improper protection and handling of PII. Identity theft is one potential consequence of insecurity. Another possible consequence is the dissemination of false information about a person, through alteration of that person's record.
- **Secondary use—**With secondary use, information about a person obtained for one purpose is used or made available for other purposes without consent.
- **Exclusion—**This is the failure to provide individuals with notice and input about their records.

10. Some potential privacy threats while disseminating information are as follows:
    - **Disclosure—**This refers to the public release of authentic personal information about an individual. The potential harm is damage to reputation or position in some form.
    - **Breach of confidentiality—**This is a disclosure that involves the violation of trust in a relationship. An example is the unauthorized release of medical information to a third party.
    - **Exposure —**This involves the exposing to others of certain physical and emotional attributes about a person, such as nude photographs or a video of an operation.
    - **Increased accessibility—**Public information is very easy to get these days, and thus this increases the likelihood of malicious use.
    - **Blackmail—**Blackmail involves the threat of disclosure. Ransomware is an example of blackmail in the cybersecurity context.
    - **Appropriation—**This involves the use of a person's identity or personality for the purpose of another.
    - **Distortion—**This refers to the manipulation of the way a person is perceived and judged by others and involves the victim being inaccurately exposed to the public. Distortion can be achieved by modifying records associated with an individual.
11. Invasion exposes the following types of threats:
    - **Intrusion—**This involves incursions into an individual's personal space. In the context of cybersecurity, intrusion is an act of penetrating into a network or a computer system and achieving some degree of access privilege to get or change some data. Intrusion is a part of a variety of security threats but can also cause a privacy threat. For example, the actual intrusion, or threat of intrusion, into a personal computer can disrupt the activities or peace of mind of the personal computer user.
    - **Decisional interference—**This techno-legal term involves the individual's interest in avoiding certain types of disclosure. To the extent that certain actions, such as registering for a government benefit, might generate data that could potentially be disclosed, the decision to perform those actions is deterred.

https://t.me/learningnets

12. Some key principles of the EU's GDPR are as follows:

- **Fair, lawful, and transparent processing—**This is very extensive and bound with legal terms. It includes, for example, an obligation to tell data subjects what their personal data will be used for.
- **Purpose limitation—**This means that personal data collected for one purpose should not be used for a new, incompatible, purpose.
- **Data minimization—**Subject to limited exceptions, an organization should only process the personal data that it actually needs to process in order to achieve its purposes.
- **Accuracy—**Personal data must be accurate and recent. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Data retention periods—**Personal data must be kept in a form viable to permit identification of data subjects for no longer than is necessary and for the purposes for which the data were collected or for which they are further processed. Data subjects hold the right to erasure of personal data at any point of time.
- **Data security—**Technical and organizational measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access.
- **Accountability—**The controller is obliged to demonstrate that its processing activities are compliant with the data protection principles.

13. NIST SP 800-53 organizes privacy controls into 8 families, with a total of 24 controls:

- **Authority and purpose—**This family ensures that organizations identify the legal bases that authorize a particular PII collection or activity that impacts privacy and specify in their notices the purpose(s) for which PII is collected.
- **Accountability, audit, and risk management—**This family consists of controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.
- **Data quality and integrity—**The objective of this family is to ensure that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used.
- **Data minimization and retention—**This family includes minimization of PII, data retention, and disposal and minimization of PII used in testing, training, and research.
- **Individual participation and redress—**This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII.

https://t.me/learningnets

- **Security—**This family ensures that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure. These controls are meant to supplement the organization's security controls that may be relevant to privacy.
- **Transparency—**This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities. This includes procedures for notifying individuals of the status of their PII and dissemination of privacy program information.
- **Use limitation—**This family ensures that the scope of PII use is limited to the intended purpose. This includes developing policies and procedures to limit internal access to PII to only those personnel who require and are authorized access, as well as similar policies and procedures for third parties outside the organization.

14. *Document* and *record* are very close in meaning but hold subtle differences when applied to information security. A document may be a record, but not all documents are records. A document is a work-in-progress object, and only authorized users can read, edit, and easily distribute it. A document is editable and therefore doesn't necessarily have to adhere to industry, government, or other regulatory standards. A record is an official file that clearly delineates terms and conditions, statements, or claims and is accepted as valid legal proof of authenticity of information.

15. The life of a record can be divided into three stages:

    1. **Active—**Here a record is used to support the organization's functions and reporting requirements. Generally, active records are referred to often during the regular course of business.
    2. **Semi-active—**Here a record is no longer needed to carry out current activities but must still be retained to meet the organization's administrative, fiscal, legal, or historical requirements.
    3. **Inactive—**Here a record is no longer required to carry out the administrative or operational functions for which it was created and is no longer retrieved or accessed. Such records can either be archived or destroyed.

16. Some supporting technologies that can be used to protect sensitive physical information are as follows:

    - Closed-circuit television (CCTV)
    - Locks
    - Alarms
    - Access control
    - Vaulting

https://t.me/learningnets

- Intelligence reports
- First responder interfaces
- Facilities management solutions
- Fire protection systems
- Time locks
- Physical access solutions

17. Following are some key issues that can help secure physical information throughout its life cycle:
    - **Identify and document—**Each item of physical information needs to be identified properly, and its existence needs to be documented.
    - **Classification—**Every physical document or other type of media (example, DVD) should be classified according to the security classification policy of the organization.
    - **Label—**An appropriate security classification label must be affixed to or incorporated into the document itself.
    - **Storage—**Secure storage is needed for all physical assets. This may be a safe, a secure area of the facility, or other physical means of restricting and controlling access.
    - **Secure transport—**If sensitive information is to be sent by a third party, such as a courier or shipping service, policies and procedures must be in place to ensure that this is done securely.
    - **Disposal—**Some kind of retention and disposal policy should be implemented across the organization for physical assets.

Chapter 7

1. ISF's SGP divides physical asset management into four topics:
    - **Hardware life cycle management—**This encompasses the management of the entire life cycle of hardware that is used to support enterprise information systems. This includes product selection, testing, deployment, assessment, and decaying.
    - **Office equipment—**This covers peripheral devices such as printers, scanners, fax machines, and multifunction devices (MFD).
    - **Industrial control systems—**This covers security issues related to systems that monitor or control physical activities such as temperature, pressure, and velocity.

https://t.me/learningnets

- **Mobile computing—**This deals with security issues related to the use of mobile devices in an enterprise information system.

2. ISF's SGP includes physical assets (for example, access gates at the entry to an office), embedded software within a physical asset (for example, embedded software on the employer's access gate), and operating systems that support any embedded software (for example, RTLinux).
3. Any organization should adopt a well-drafted hardware life cycle management policy, considering the following reasons:
   - The hardware asset should be retained until the cost of operating it is lower than the cost of low productivity, increased downtime, worker safety, and elevated levels of user dissatisfaction. A systematic approach to life cycle management can provide guidance on when to replace particular equipment.
   - Organizations not following any hardware asset management are often frustrated by the communication gaps that allow assets to be lost, acquisitions to be made when spares are in the warehouse, or upgrades failing due to incomplete information. All this swells operation cost and hits the top business line.
   - Hardware life cycles are vendor dependent; some vendors might follow a three-year cycle, while others might follow a five-year cycle. Hence, the organization should centralize this information in a configuration management database (CMDB).
   - Every hardware asset brings its own set of threats. An organization can reduce risk by having and using the tools to properly track and manage its hardware.
   - There is a need to map hardware with the applications installed on that hardware for software compliance management and reporting. For example, the organization should know how many bar code readers were not used for past three months and what version of firmware is installed on them to prepare for upgrade.
4. An organization should follow these steps to acquire any hardware asset:
   1. **Request and approval—**This includes application of standards, redeployment, and initiation of a purchase, if appropriate.
   2. **Vendor relationships—**This includes creation of contracts and management of vendor relationships.
   3. **Acquisition—**This includes contract negotiations and contract execution.
   4. **Receipt—**This triggers initiating payment of invoices and creating an incident to configure and deliver to the correct individual/location/department.
5. After deployment, equipment can be managed in several ways:
   - The best way to maintain it is by doing preventive maintenance. Depending on the nature of the work, usage, and asset type, proper monitoring must be done and, based on that, the service schedule should be decided.

https://t.me/learningnets

- Another way is to track key hardware assets. Technology such as RFID and geotagging can help organizations ensure that critical assets, such as essential information system components, remain in authorized locations.
- All hardware must be properly monitored and measured on all key parameters.
- Hardware should be serviced on a regular basis, and it must be assessed on safety norms after each service.

6. There are three potential vulnerability sources in an MFD:
   - **Print, fax, and copy/scan logs—**With print logs, there is the threat of exposure of sensitive document names, network usernames, and URLs of websites users have printed from. Fax numbers indicate with whom an organization does business, and long-distance codes/long-distance credit-card numbers may show up with dialed numbers. Copy/scan logs can expose email addresses of recipients and logon information for FTP file uploads.
   - **Address books—**Some MFDs allow the user to create address books as distribution or destination lists. This may expose internal and customer email addresses and fax numbers, long-distance codes and credit-card numbers, and server addresses and usernames for FTP sites.
   - **Mailboxes—**Mailboxes are used to store scans, faxes, or templates on an MFD. Unless it is password protected, a mailbox could provide an attacker with entire faxes or scanned documents containing sensitive information.
7. Media sanitization a process of rendering access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. Three increasingly secure actions for sanitization are defined:
   - **Clear—**Here you apply logical techniques to sanitize data in all user-addressable storage locations for protection against simple noninvasive data recovery techniques; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
   - **Purge—**Here you apply physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques. This can be achieved by performing multiple overwrites. For a self-encrypting drive, cryptographic erasure can be used. If the drive automatically encrypts all user-addressable locations, then all that is required is to destroy the encryption key, which could be done with multiple overwrites.
   - **Destroy—**This method renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. Typically the medium is pulverized or incinerated at an outsourced metal destruction or licensed incineration facility.

https://t.me/learningnets

8. The elements of an ICS are as follows:

   - **Sensor—**A sensor measures some phenomenon of a physical, chemical, or biological domain and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal.
   - **Actuator—**An actuator receives an electronic signal from a controller and responds by interacting with its environment to induce a change in behavior of a physical, chemical, or biological entity.
   - **Controller—**The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. The controller is devoid of intelligence and needs a human–machine interface for direction.
   - **Human–machine interface—**Operators and engineers use human interfaces to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The human interface also gives GUI displays about status and health of the system.
   - **Remote diagnostics and maintenance—**Diagnostic and maintenance utilities are used to prevent, identify, and recover from abnormal operations or failures.

9. An IT system is non-real time, whereas an ICS is hard real time. IT systems need a consistent response and tolerate some delay, but an ICS wants responses under scheduled time. High delay and jitter are not acceptable for an ICS, whereas they may be acceptable in an IT system. IT systems are not usually designed for critical emergency responsiveness, and usually an ICS is designed for that very reason. Finally, security can restrict access to an IT system and may affect its functionality, whereas an ICS need to be strictly controlled but not at the expense of hampering its functionality.

10. Some common security threats to an ICS are as follows:

    - Disruption of service due to blocked or delayed flow of information through ICS networks.
    - Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment; create environmental impacts; and/or endanger human life.
    - Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects.
    - ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.

https://t.me/learningnets

- Financial losses due to interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Danger to human life due to interference with the safety operation.

11. A typical mobile device technology stack has four layers:

- **Hardware—**The base layer of the technology stack is termed hardware. This includes an application processor and a separate processor that runs the cellular network processor, typically referred to as the baseband processor. There are other chips, such as system clock, Wi-Fi controller, and USB controller. Further, there may be hardware-encryption modules and other security modules. The hardware layer also includes the peripherals incorporated into the device, such as a camera and SIM card. Vulnerabilities at this level can serve as attack vectors.
- **Firmware—**The firmware is needed to boot the mobile operating system (that is, the boot loader) and verify additional device initialization code, device drivers used for peripherals, and portions of the mobile operating system prior to the user actually using the device.
- **Mobile operating system—**Common operating systems for the mobile device are Android, iOS, and Symbian. The operating system lies between hardware and applications and helps the applications perform. It also isolates third-party applications in some manner to prevent unexpected or unwanted interaction between the system, its applications, and the applications' respective data (including user data). Vulnerabilities are routinely discovered in mobile device operating systems. However, the development of patches and the update of the software are beyond the control of the enterprise and in the hands of the operating system provider.
- **Application—**This layer includes third-party applications, utility apps, games, and services provided by the mobile device vendor and facilities for defining permissions.

12. According to SP 800-14, major security concerns for mobile devices are as follows:

- **Lack of physical security controls—**Mobile devices are mostly under the complete control of the user (password protection, biometric lock) and are used and kept in a variety of locations outside the organization's control, such as employee's home. Even if a device is required to remain on premises, the user may move the device within the organization between secure and insecure locations, thereby exposing it to theft and tampering threats. The threat is twofold: A malicious party may attempt to recover sensitive data from the device itself or may use the device to gain access to the organization's resources
- **Use of untrusted mobile devices—**Apart from official assets, virtually all employees have personal smartphones and/or tablets. The organization must assume that these devices are not trustworthy; the devices may not employ encryption and either the user or a third party may have installed a bypass to the built-in restrictions on security, operating system use, and so on.

https://t.me/learningnets

- **Use of untrusted networks—**An employee's mobile device can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from there to the organization. Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks.
- **Use of applications created by unknown parties—**It is very convenient to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software since the user unintentionally may give complete access to mobile/PDA data to the new app.
- **Interaction with other systems—**All smartphones and tablets can automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage without paying much attention to security aspects. Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, and there is also a risk of the introduction of malware.
- **Use of untrusted content—**Mobile devices may access and use content in unique ways. Here the vulnerability is twofold: The content is untrustable, and the access method is not foolproof. An example is the Quick Response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. A QR code translates to a URL, and a malicious QR code could direct mobile devices to malicious websites.
- **Use of location services—**The GPS capability on mobile devices can be used to track the physical location of the device to the nearest cell. This can be a security risks as an attacker can use the location information to determine where the device and user are located, which may be of use to the attacker.

13. NIST has developed a tool called AppVet that provides automated management support of the app testing and app approval or rejection activities. AppVet facilitates the app vetting workflow by providing an intuitive user interface for submitting and testing apps, managing reports, and assessing risk.

Chapter 8

1. The initiation phase typically consists of the following tasks:
   - **Strategy—**This task involves ensuring that the system release is fully aligned to all master strategy and intent.
   - **Research—**This task involves determining opportunities and solution options that meet requirements.

https://t.me/learningnets

- **Feasibility—**This task involves ensuring that if the overall strategy is acceptable to management, then the team takes the next step to examine the viability of the system in terms of economic, financial, technology, operations, social, and organization factors.
- **Planning—**This task includes activities such as detailing what will actually go into the systems release (for example, new features and break-fixes), creating initial project plans, and improving budget estimates.
- **Requirements—**This task is primarily focused on developing the requirements specification of what needs to be accounted for in downstream design and implementation activities.

2. The development/acquisition phase typically involves two types of testing:
   - **Integration testing—**This type of testing takes as scope all interfaces of the system (to other entities). Here all data and technology connections are tested for a specific system moving through the SDLC and all its upstream system dependencies (user layer) and all its downstream system targets (service layer).
   - **User acceptance testing—**This takes as scope the entire system and tests system functions that end users will be able to execute while operating in the final production environment.
3. The changeover is implemented by running the new system with the data from one or more of the previous periods for the whole system or part of it. The results are compared with the old system results, and the old system is replaced if and only if the results prove better. It is less expensive and risky than the parallel run approach. This strategy builds confidence, and the errors are traced easily, without affecting the operations at all.
4. The DevOps methodology rests on the joint effort of all participants—including business unit managers, developers, operations staff, security staff, and end user groups—in creating a product or system collaborating from the beginning. DevOps can be defined as the practice of operations and development engineers participating together in the entire service life cycle, from design through the development process to active production support. The techniques can range from using source control to debugging to testing and to participating in an Agile development process.
5. Major stages in the life cycle of an application/system are as follows:
   1. **Development—**Developers build and deploy code in a test environment, and the development team tests the application at the most basic level. The application must meet certain criteria for advancement to the next phase.
   2. **System integration testing—**The application is tested to ensure that it works with existing applications and systems. The application must meet the criteria of this environment before it can move to the next phase.

https://t.me/learningnets

3. **User acceptance testing—**The application is tested to ensure that it provides the required features for end users. This environment is usually production-like. The application must pass these requirements to move to the next phase.
4. **Production—**The application is made available to users. Feedback is captured by monitoring the application's availability and functionality. Any updates or patches are introduced in the development environment to repeat this cycle.

6. The four phases of the DevOps reference architecture are as follows:
    1. **Plan and measure—**This activity focuses on business units and their planning process. The planning process relates business needs to the outcomes of the development process. This activity can start with small, limited portions of the overall plan, identifying outcomes and resources needed to develop the required software. The plan must include developing measures that are used to evaluate software, adapt and adjust continually, relate to customer needs, and continually update the development plan and the measurement plan.
    2. **Develop and test—**This activity focuses on collaborative development, continuous integration of new code, and continuous testing of the system. It focuses on catching the synergies of development and testing teams. Useful tools are automated tracking of testing against measured outcomes and virtualized test beds that enable testing in an isolated but real-world environment.
    3. **Release and deploy—**This activity provides a continuous delivery pipeline that automates deployment to test and production environments using variety of tools. Releases are managed centrally in a collaborative environment that leverages automation. Deployments and middleware configurations are automated and then matured to a self-service model that gives individual developers, teams, testers, and deployment managers the capability to continuously build, provision, deploy, test, and promote.
    4. **Monitor and optimize—**This activity includes the practices of continuous monitoring, customer feedback, and optimization to monitor how applications are performing, allowing businesses to adapt their requirements as needed.
7. The two key foundations on which DevOps rests are collaboration and automation. Collaboration begins with management policy to encourage and require the various actors in the software development and deployment process to work together. Automation consists of tools that support that collaboration and are designed to automate as much as possible this cyclic process.
8. Control gates are decision points at the end of each phase when the system needs be evaluated and management needs to determine whether the project should continue as is, change direction, or be discontinued. Typical examples of control gates are performance review, code review, and financial feasibility analysis.

https://t.me/learningnets

9. Key security considerations that exist throughout the SDLC are as follows:
   - **Secure concept of operations—**There should be an operations or business continuity document for secure development that contains a contingency plan for the code repository as well as documents as both are the predominant work products of software and system development and should be preserved in the event of interruption to the development environment.
   - **Standards and processes—**These play the role of a guide and help decide and document appropriate security processes for the assurance level required by the system.
   - **Security training for development team—**Additional security training may be needed for key developers to understand the current threats and potential exploitations of their products as well as training for secure design and coding techniques, based on the prevailing standards and need.
   - **Quality management—**This includes planning, assurance, and control that are keys to ensuring minimal defects in and proper execution of the information system.
   - **Secure environment—**The development environment**—**including workstations, servers, network devices, and code repositories**—**needs to meet the organization's security requirements. A secure development environment is a prerequisite for developing secure software and systems.
   - **Secure code practices and repositories—**These should be religiously followed. Special attention should be placed on code repositories, with an emphasis on systems that support distributed code contribution with check-in/check-out functionality. Role-based access should apply to accessing the code repository, and logs should be reviewed regularly as part of the secure development process. When possible, completed software components that have passed security certification should be retained as reusable components for future software development and system integration.
10. Some of the control gates at the development/acquisition phase are as follows:
    1. **Architecture/design review—**Here you do review of the security architecture and design that evaluates its integration with other systems and the overall enterprise architecture.
    2. **Performance review—**Here you evaluate whether the system meets the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use.
    3. **Functional test review—**Here you ensure that functional requirements are sufficiently detailed and are testable after deployment.
    4. **Risk management review—**Here you review the risk management decisions made up to that point and their impact on the system or its security controls.
    5. **Mid-project status and financial review—**Here you determines if there have been changes in the planned level of effort and evaluate the effect on costs and benefits.

https://t.me/learningnets

11. The key activities for disposal phase are:
    - **Create disposal/transition plan—**This plan makes all stakeholders aware of the future plan for the system and its information. The plan should document all the planned steps for disposal.
    - **Ensure information protection—**Any information that is to be archived or otherwise retained must be accessible by appropriate hardware in the future. If the information is encrypted, appropriate key management functions must be invoked.
    - **Sanitize media—**The procedures of SP 800-88 or similar standards should be followed to ensure thorough sanitization.
    - **Dispose of hardware and software—**Hardware and software can be sold, given away, destroyed, or discarded, as provided by applicable law or regulation.
    - **Close system—**The information system is formally shut down and disassembled at this point.
12. According to the International Foundation for Information Technology, best practices for managing the SDLC are as follows:
    - **Ownership—**Assign full, unambiguous accountability for system development management to key individuals, committees, or departments.
    - **Inventory—**Religiously maintain a central database of all items related to the management of system development, including requirements, deliverables, and the status of control gates.
    - **Terminology—**Be consistent in the use of standard terminology for the various aspects of system development.
    - **Data centralization—**Maintain core data**—**that is, data that is required by or is useful for stakeholders involved in system development in a central repository.
    - **Metrics—**Ensure that management discuss and agree on a set of performance metrics that can be defined, tracked, and analyzed to assess progress in system development.
    - **Standards and best practices—**Follow, to the maximum extent possible, industry standards and best practices for system development. This helps in interoperability and legal compliance.
    - **Transparency—**Strive to make any and all system development management data transparent to all other appropriate stakeholders, at a minimum, and often to the entire enterprises.
13. The International Foundation for Information Technology defines the following environments for system development:
    - **Research—**This environment is used as an isolated sandbox for researching the viability of technologies and solutions, often implemented in the form of a proof of concept, a study, or an experiment.

https://t.me/learningnets

- **Developer work space—**This environment accommodates the activities associated with the private or localized implementation that is performed by a single or individual resource, such as a software coder or an engineer, to provide an isolated working area that provides the flexibility to work freely without interference with or from other environments where other resources may be working.
- **Centralized build—**This environment accommodates the activities associated with centralized or merged builds. In this environment, the individual developer products are brought together to create a single, unified build.
- **Integration testing—**An isolated environment is used to test the integrations (that is, the data communications connections, channels, and exchanges) between the product, system, or software release being worked on and those of other products, systems, or instances of software that the release is intended to work with and communicate with during its operation in other downstream environments, such as production.
- **User acceptance testing—**This environment enables human interaction with the system for the purpose of obtaining final approval and sign-off for the features and functions of the release.
- **Production—**This environment is the final targeted environment where a product, system, or software release operates for business use. This environment is deemed to be the most critical, as failures in this environment can potentially disturb or even shut down a line of business, depending on the importance of the product, system, or software being used by its end users.

Chapter 9

1. Application management (AM), in a nutshell, is the process of managing the operation, maintenance, versioning, and upgrading of an application throughout its life cycle. It includes best practices, techniques and procedures that are critical for any deployed application's optimal operation, performance, and efficiency throughout the enterprise and back-end IT infrastructure.
2. The key stakeholders of application management are as follows:
   - **Application owners—**These are key business executive personnel who view AM in terms of business productivity, revenue, and control.
   - **Application developers/managers—**These are key IT enterprise personnel responsible for application development, deployment, and maintenance.
   - **Application testers—**These are key IT enterprise personnel responsible for testing, validating, and certifying an application for production.

https://t.me/learningnets

- **Application users—**These are end users of an application. For them, AM is measured according to security, privacy, versioning, and overall control of application processes and modules.

3. Application life cycle management typically has following stages.
    1. **Gather requirements—**Here the business units identify the functional and business process requirements for the change or new application.
    2. **Design—**In this phase, the design team translates the requirements into a technical solution. IT infrastructure planners, solution architects, and so on typically get involved at this step, and simulation tools help them effectively assess long-term requirements. This ensures that IT infrastructure resources are available to support ongoing operations of the new application.
    3. **Build, integrate, test—**In this phase, all the components and flows are developed and tested both individually and in integration with the system to uncover any functional and process flaws. Detecting adverse impacts early in the development process helps developers take appropriate actions quickly.
    4. **Implement, deploy—**This covers the rollout of the new application. The application modules are first put into production libraries. Then any customer training required to effectively and efficiently use the new facilities is provided.
    5. **Operate—**Here you monitor and measure the application in the following areas:
        - Addressing changes in regulatory requirements
        - Fixing flaws uncovered in the application
        - Monitoring service levels (and addressing problems in missed service levels)
        - Measuring and reporting on application performance
    6. **Optimize—**Here IT management uses past measurement and in-house heuristics to seek ways to optimize existing applications. Areas of concern include performance, capacity utilization, and user satisfaction and productivity.
4. Total cost of ownership (TCO), in a generic sense, is an analysis to determine all the lifetime costs that follow from owning certain kinds of assets. From an applications point of view, it is a detailed analysis of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses, and the opportunity costs of downtime, training, and other productivity losses.
5. According to Gartner, an effective APM strategy consists of following steps:
    1. **End-user experience monitoring—**The first step is to capture both qualitative and quantitative elements of user experience. It is a precursor to determining how end-to-end performance impacts the user and identifies any problem. This step is the most important.

https://t.me/learningnets

2. **Runtime application architecture discovery, modeling, and display—**The second step is to study the software and hardware components involved in application execution, as well as their communication paths, to establish the potential scope of the problem. In this step, you get to know the specific components (hardware or software) fueling the application's performance. For example, a database server may be broken down into components such as processor, memory, disk, query execution time, and so forth.
3. **User-defined transaction profiling—**In this step, you record user-defined transactions and analyze them to identify the source of the problem. Here the concern is not so much with the total transaction time but rather with what portions of the application are spending time processing the transaction.
4. **Component deep-dive monitoring in an application context—**The fourth step is about conducting deep-dive monitoring of the resources consumed by and events occurring within the components found in step 2.
5. **Analytics—**Finally, you use analytics to crunch the data generated in the first four steps, discover meaningful and actionable patterns, pinpoint the root cause of the problem, and ultimately anticipate future issues that may impact the end user.

6. COTS stands for commercial-off-the-shelf (COTS), and it refers to a software or hardware item that is commercially available for leasing, licensing, or sale to the general public in its original form, without any (major) need for a modification or maintenance over the life cycle of the product to meet the needs of the procuring agency (for example, Windows 10, MATLAB, or BlueJ IDE for Java development).

7. ModSecurity is an open source software web application firewall (WAF). A WAF is a firewall that monitors, filters, or blocks data packets as they are transiting from a web application. It can be run as a standalone server in a premises network or as a server plug-in or as a cloud service. The key role of a WAF is to inspect each packet and use a rule table (application logic) to analyze and filter out potentially harmful traffic.

   Some of its salient features are as follows:

   - **Real-time application security monitoring and access control—**Full-duplex HTTP traffic sieves through ModSecurity, where it is thoroughly inspected and filtered. ModSecurity also has a persistent storage mechanism, which enables tracking of events over time to perform event correlation.
   - **Virtual patching—**This is the ability to apply web application patching without making any direct modifications to the application. Virtual patching is applicable to applications that use any communication protocol, but it is particularly useful with HTTP because the traffic can generally be well understood by an intermediary device.
   - **Complete bidirectional HTTP traffic logging—**Unlike many other web services, ModSecurity has the ability to log events, including raw transaction data, which is

https://t.me/learningnets

essential for forensics. In addition, the system manager gets to choose which transactions are logged, which parts of a transaction are logged, and which parts are sanitized.

- **Web application hardening—**This is a method of attack surface reduction in which the system manager selectively narrows down the HTTP features that will be accepted (for example, request methods, request headers, and content types).

8. Some of the benefits of EUDAs are as follows:

   - **Convenience and ease of use—**EUDAs can be developed easily and quickly by non-IT staff to meet the requirements of the end users. EUDAs allow businesses and users to quickly deploy solutions in response to shifting market and economic conditions, industry changes, or evolving regulations.
   - **Powerful tools and technology-aware end users—**End-user tools offer rich functionality, including the ability to connect to corporate data sources. As a result, technology-savvy users can perform powerful data processing from their desktops. This can help plug functionality gaps for business systems.
   - **Demand for more and more information—**Traditionally, managers were often constrained by standard reports in IT systems that failed to meet all management information and reporting requirements. The lack of flexibility in these systems and increasing demand for different views of the data have resulted in an increase in the level of end-user computing in organizations.

9. There are a number of disadvantages and risks to EUDAs:

   - **Errors—**Errors can occur at nearly any stage, such as at data entry, within formulas, within application logic, or with links to other applications or data sources. Without a sound SDLC discipline, such errors are bound to occur, and they could result in poor decision making or inaccurate financial reporting.
   - **Poor version and change control—**EUDAs do not follow a standard method of development and thus they can be more difficult to control than more traditional IT-developed applications.
   - **Poor documentation—**EUDAs generally have very poor or no documentation. Files that have not been properly documented may be used incorrectly after a change in ownership of the EUDA, or they may just be improperly used in general. Again, this can lead to unintended and undetected errors.
   - **Lack of security—**Users are more interested in getting their problems solved than in evaluating security. Hence, they generally exchange files in an insecure manner. This can lead to increased errors, or it might allow sensitive and confidential information to be seen by unauthorized users. An EUDA could possibly be used to perpetuate fraud or hide losses.

https://t.me/learningnets

- **Lack of audit trail—**EUDAs are mostly unaudited. The ability to audit and control changes to key data is essential both for internal governance and for compliance with external regulation. For critical applications, managing this risk effectively is crucial and in many instances requires monitoring and controlling changes at a detailed level.
- **Regulatory and compliance violations—**A host of regulations deal with security and privacy for which the enterprise is responsible.
- **Unknown risk—**The greatest operational risk with the use of EUDAs is not knowing the magnitude and severity of a potential problem. The use of EUDAs is so widespread that it may be extremely difficult to assess just how many exist, how many are used in critical business applications, how they are linked together, and where data is fed into or extracted from other IT applications. To quantify this risk, it is necessary to carry out a full inventory of EUDA usage and a detailed risk assessment of all business-critical spreadsheets.
- **Opportunity cost—**Scarce resources (money or employee time) may be wasted on developing these applications, which would otherwise be utilized in work that provides a financial returns.

10. There are four key elements of the EUDA security framework:

- **Governance—**As part of good governance, senior executives must define what constitutes a EUDA. This involves distinguishing EUDAs from IT-developed and supported applications and specifying which types of EUDAs should be placed under management control.
- **People—**It is the duty key stakeholders to properly manage and control EUDAs, and thus there should be a proper process to identify them. Once the key stakeholders are identified, the next step is to establish the roles and responsibilities. Stakeholder roles include the program sponsor, central program group, steering committee, business unit representatives, EUDA users, and internal auditors.
- **Process—**There should be a proper process for assessing the security of an EUDA. Management's top concern with respect to EUDAs is the potential risks of any given application. For each EUDA, the EUDA owner can apply a risk model to determine which EUDAs should be placed under formal management control. Furthermore, there should be an inventory or register of all EUDAs that are under management control, with details concerning the application, including security-related aspects.
- **Technology—**From a technology point of view, an organization should perform an assessment to identify tools and techniques needed to support the development of EUDAs. Specific EUDA management software tools can be deployed, or native functionality (such as Microsoft SharePoint) can be used; various degrees of functionality are available in different products.

https://t.me/learningnets

Chapter 10

1. The term AAA stands for authorization, authentication, and access control. Authorization implies granting of access rights of system resources to a user, program, or process. Authorization comes after successful authentication and defines possible actions for an authenticated user or agent. Authentication is the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Access control is the process of granting or denying specific requests, such as accessing and using information and related information processing services and or entering specific physical facilities.
2. There are two main functions involved in user authentication:
   - **Identification—**This involves presenting an identifier to the security system to verify the identity with respect to the system.
   - **Verification—**This involves presenting or generating authentication information that corroborates the binding between the entity and the identifier.
3. The NIST 800-63 digital identity model involves three pivotal concepts:
   - **Digital identity—**The digital identity is the unique representation of a subject engaged in an online transaction. The representation consists of an attribute or set of attributes that uniquely describe a subject within a given context of a digital service but does not necessarily uniquely identify the subject in all contexts.
   - **Identity proofing—**This process establishes that a subject is who he or she claims to be to a stated level of certitude. This process involves collecting, validating, and verifying information about a person.
   - **Digital authentication—**This process involves determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate.
4. NIST's digital identity model involves six entities:
   - **Credential service provider (CSP)—**This refers to a trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.
   - **Verifier—**This refers to an entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators, using an authentication protocol.
   - **Relying party (RP)—**This refers to an entity that relies on the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

https://t.me/learningnets

- **Applicant—**This refers to a subject undergoing the processes of enrollment and identity proofing.
- **Claimant—**This refers to a subject whose identity is to be verified using one or more authentication protocols.
- Subscriber**—**This refers to a party who has received a credential or an authenticator from a CSP.

5. There are three authentication factors in user identity authentication:
   - **Knowledge factor—**This is something that is partly or fully known by an individual. It requires the user to demonstrate knowledge of hidden information. Normally, it is used in single-layer authentication processes in the form of passwords, passphrases, PINs, or answers to secret questions. Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions.
   - **Possession factor—**This is something possessed by the individual. It is normally a physical entity possessed by the authorized user to connect to the client computer or portal. This type of authenticator is referred to as *hardware token*, of which there are two types. Connected hardware tokens are items that physically connect to a computer in order to authenticate identity, and disconnected hardware tokens are items that do not directly connect to the client computer but instead require input from the individual attempting to sign in.
   - **Inherence factor—**This is something intrinsically present in the individual. It refers to the characteristics, called biometrics, that are unique or almost unique to the individual. These include static biometrics, such as fingerprint, retina, and face; and dynamic biometrics, such as voice, handwriting, and typing rhythm.
6. Common attacks on password-based authentication along with their mitigation steps are as follows:
   - **Offline dictionary attack—**In this type of attack, an attacker bypasses system controls and gains access to the password file. The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by using that ID/password combination. Countermeasures include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords in the event that the password file is compromised.
   - **Specific account attack—**This is a variation of the preceding attack type, but here the attacker uses a popular password and tries it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess. Countermeasures include policies to inhibit the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns.

https://t.me/learningnets

- **Password guessing against a single user—**Here the attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password. Countermeasures include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, minimum length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed.
- **Workstation hijacking—**Here the attacker waits until a logged-in workstation is unattended. The standard countermeasure is automatically logging the user out of the workstation after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.
- **Exploiting user mistakes—**This type of attack exploits users' mistakes. A user may intentionally share a password to enable a colleague to share files, for example. Also, attackers are frequently successful in obtaining passwords by using social engineering tactics that trick the user or an account manager into revealing a password. Countermeasures include user training, intrusion detection, and simpler passwords combined with another authentication mechanism.
- **Exploiting multiple password use—**Here the attacker can harm more than one system as the user has set the same password for multiple systems. Countermeasures include a policy that forbids using the same or similar password on particular network devices.
- **Electronic monitoring—**Here the attack can snoop the network traffic to extract a password that is transmitted over a network. Simple encryption will not fix this problem because the encrypted password is, in effect, the password and can be observed and reused by an adversary.

7. The salt value serves three purposes in terms of hashing:
   - It makes duplicate passwords invisible in the password file. Even if two users choose the same password, those passwords will be assigned different salt values. Hence, the hashed passwords of the two users will differ.
   - It makes offline dictionary attacks significantly difficult. For a salt of length b bits, the number of possible passwords is increased by a factor of 2b, increasing the difficulty of guessing a password in a dictionary attack because and exponential order algorithm takes years of computation to solve.
   - It becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them.
8. The major vulnerabilities of password file protection are as follows:
   - A hacker may be able to exploit a software vulnerability in the operating system to bypass the access control system long enough to extract the password file. Alternatively, the hacker may find a weakness in the file system or database management system that allows access to the file.

https://t.me/learningnets

- An accident of protection or a manual slip might render the password file readable, thus compromising all the accounts.
- Some users may have accounts on other machines in other protection domains, for which they might use the same password. Thus, if the passwords could be read by anyone on one machine, a machine in another location might be compromised.
- A lack of or weakness in physical security may aid a hacker. Sometimes there is a backup to the password file on an emergency repair disk or archival disk. Access to this backup enables the attacker to read the password file. Alternatively, a user may boot from a disk running another operating system such as Linux and access the file from that operating system.
- Instead of capturing the system password file, another approach to collecting user IDs and passwords is through sniffing network traffic when a user is trying to log in to an unsecured channel.

9. The potential drawbacks of using a memory card as an authentication device are as follows:
   - **Requirement of special reader—**this Increases the cost of using the hardware token and creates the requirement to maintain the security of the reader's hardware and software.
   - **Hardware token loss—**This event can temporarily prevent the owner of a lost token from gaining system access. Thus, there is an administrative cost in replacing the lost token. In addition, if the token is found, stolen, or forged, then an adversary now need only determine the PIN to gain unauthorized access.
   - **User dissatisfaction—**Users may find using memory cards for computer access inconvenient, unnecessary, and futile.
10. You can categorize authentication protocols used in a smart grid in the following manner:
    - **Static—**With a static protocol, the user authenticates himself or herself to the token, and then the token authenticates the user to the computer. The latter half of this protocol is similar to the operation of a memory token.
    - **Dynamic password generator—**Here both the token and the computer system are actively involved. The token generates a unique password periodically—say every minute. This password is then entered into the computer system for authentication, either manually by the user or electronically via the token. The token and the computer system must be initialized and kept synchronized so that the computer knows the password that is current for this token.
    - **Challenge-response—**In this case, the computer system generates a challenge, such as a random string of numbers. The smart token generates a response based on the challenge.
11. A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. OTP tokens are usually

https://t.me/learningnets

pocket-size fobs with a small screen that displays a number. The number changes periodically, say every 30 or 60 seconds, depending on how the token is configured. An OTP is more secure than a static password and has the potential to replace authentication login information or may be used to add another layer of security.

12. Possible threats to possession-based authentication are as follows:

    - **Theft—**An attacker can steal a token device. If a second factor is required, such as a PIN, the attacker must also use some means to obtain or guess the PIN. If the second factor is biometric, the attacker must come up with some way of forging the biometric characteristic.
    - **Duplication—**The attacker gains access to the device and clones it. Again, if a second factor is required, the attacker's task is more formidable.
    - **Eavesdropping/replaying—**The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating. This captured information can be used later. If there is a time-sensitive aspect to the exchange, such a nonce or the use of an OTP, this latter attack can be thwarted.
    - **Replay—**If the attacker can interpose between the token device and the server, this constitutes a man-in-the-middle attack, in which the attacker assumes the role of the client to the server and the server to the client.
    - **Denial of service—**The attacker makes repeated failed attempts to access the server, which may cause the server to lock out the legitimate client.
    - **Host attack—**The attacker may gain sufficient control of the authentication server to enable the attacker to be authenticated to an application.

13. A biometric authentication system uses unique physical characteristics of an individual to authenticate the user. These include static characteristics, such as fingerprints, hand geometry, facial characteristics, and retinal and iris patterns; and dynamic characteristics, such as voiceprint, signature, and gait movement. Internally biometrics is based on pattern recognition, and biometric authentication is both technically complex and expensive compared to other methods.

14. Major criteria in designing a biometric system are as follows:

    - **Universality—**A very high percentage of the population should have the characteristic. For example, virtually everyone has recognizable fingerprints, but there are rare exceptions.
    - **Distinctiveness—**No two people should have identical characteristics. For some otherwise acceptable characteristics, identical twins share virtually the same patterns, such as facial features and DNA, but not other features, such as fingerprints and iris patterns.

https://t.me/learningnets

- **Permanence—**The characteristic should not change with time. For otherwise acceptable characteristics, such as facial features and signatures, periodic reenrollment of the individual may be required.
- **Collectability—**Obtaining and measuring the biometric feature(s) should be easy, non-intrusive, reliable, and robust, as well as cost-effective for the application.
- **Performance—**The system must meet a required level of accuracy, perform properly in the required range of environments, and be cost-effective.
- **Circumvention—**The difficulty of circumventing the system must meet a required threshold. This is particularly important in an unattended environment, where it would be easier to use such countermeasures and a fingerprint prosthetic or a photograph of a face.
- **Acceptability—**The system must have high acceptance among all classes of users. Systems that are uncomfortable to the user, appear threatening, require contact that raises hygienic issues, or are non-intuitive are unlikely to be acceptable to the general population.

15. The false match rate (FMR) is an important measure of biometric authentication system performance. The FMR is the rate at which a biometric process mismatches biometric signals from two distinct individuals as coming from the same individual.

16. Presentation attack detection (PAD) involves methods created to directly counter spoof attempts at the biometric sensor and are of two kinds: artifact detection and liveness detection. Artifact detection attempts to determine the originality of the sample. For example, for a voice detector, an artificial detector will attempt to determine if it is a human voice or produced by a voice synthesizer. Liveness detection attempts to determine the actuality of the sample. For instance, it will answer the question "Is the biometric sample at the sensor from a living human presenting a sample to be captured?" For example, is it a fingerprint sensed from the user's finger, or is it a fingerprint presented by the lift of a fingerprint onto a printed surface?

17. NIST SP 800-63 provides a useful way of characterizing the risk of an authentication system by using the concept of authentication assurance level (AAL). The AAL describes the degree of confidence in the registration and authentication processes. A higher level of AAL indicates that an attacker must have better capabilities and expend greater resources to successfully subvert the authentication process.

18. There are three levels of AAL.

    1. **AAL1—**This level provides some assurance that the claimant controls an authenticator bound to the subscriber's account. It requires either single-factor or multifactor authentication, using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

https://t.me/learningnets

2. **AAL2—**This level provides high confidence that the claimant controls the authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s).
3. **AAL3—**This level provides very high confidence that the claimant controls the authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication requires use of a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance.

19. An out-of-band device is a physical device with a unique address and that can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this secondary channel, separate from the primary channel for e-authentication.

20. Customer access refers to the access to business applications by individuals such as end users of an online ecommerce site, or subcontractors of a manufacturing companies, or vendors of a semiconductor company. Customer access presents additional considerations and security challenges beyond those involved with system access for employees. Before providing customers with access to specific applications and information resource, a risk assessment needs to be carried out and the required controls identified. An individual or a group within the organization should be given responsibility for authorizing each customer access arrangement. Furthermore, there should be approved contracts between the organization and the customer that cover security arrangements. Any customer access to system resources should be subject to the same types of technical controls as with employees. It is a big legal and ethical responsibility of an organization to protect data about the customer.

Chapter 11

1. According to SGP, system management is divided into two areas: system configuration and system maintenance. The objective of *system configuration* is to develop and enforce consistent system configuration policies that can cope with current and protected workloads and protect systems and the information they process and store against malfunction, cyber attack, unauthorized disclosure, and loss. The objective of *system maintenance* is to provide guidelines for the management of the security of systems by performing backups of essential information and software, applying a rigorous change management process, and monitoring performance against agreed service level agreements.

2. NIST SP 800-123 mentions the following common security threats to servers:

   - Malicious entities may exploit software bugs in the server or its underlying operating system to gain unauthorized access to the server. Further, they may attack other entities after compromising a server. These attacks can be launched directly (for example, from the compromised host against an external server) or indirectly (for example, placing

https://t.me/learningnets

malicious content on the compromised server that attempts to exploit vulnerabilities in the clients of users accessing the server).

- Denial-of-service (DoS) attacks may be directed to the server or its supporting network infrastructure, denying or hindering valid users from making use of its services.
- Sensitive information on the server may be read by unauthorized individuals or changed in an unauthorized manner.
- Sensitive information transmitted unencrypted or weakly encrypted between the server and the client may be intercepted.
- Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the server.

3. The SANS Institute describes the following general requirements for server security:
   - All internal servers deployed at the organization must be owned by an operational group that is responsible for system administration.
   - Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the CISO.
   - Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the CISO. Specifically, the following items must be met:
     - Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
       - Server contact(s) and location and a backup contact
       - Hardware and operating system/version
       - Main functions and applications, if applicable
     - Information in the corporate enterprise management system must be kept up-to-date.
     - Configuration changes for production servers must follow the appropriate change management procedures.
4. Virtualization is the process of creating a non-real (or virtual) representation of an entity. It is a technology that provides an abstraction of the computing resources used by some software, which thus runs in a simulated environment called a virtual machine (VM). Virtualization improves efficiency in the use of the physical system resources compared to what is typically seen using a single operating system instance. Virtualization can also provide support for multiple distinct operating systems and associated applications on the one physical system. It can be a very cost-effective solution to a firm that wants to launch its product in a short time and on a small budget.

https://t.me/learningnets

5. A hypervisor is software that runs on top of hardware and gives services to the VMs by acting as a resource broker. It allows multiple VMs to safely coexist on a single physical server host and share that host's resources. The virtualizing software provides abstraction of all physical resources (such as processor, memory, network, and storage) and thus enables multiple computing stacks, called virtual machines, to be run on a single physical host. Principal functions of hypervisor are as follows:

   - **Execution management of VMs—**This includes scheduling VMs for execution, virtual memory management to ensure VM isolation from other VMs, and context switching between various processor states. It also includes isolation of VMs to prevent conflicts in resource usage and emulation of timer and interrupt mechanisms.
   - **Device emulation and access control—**This is all about emulating all network and storage (block) devices that different native drivers in VMs are expecting, mediating access to physical devices by different VMs.
   - **Execution of privileged operations by hypervisor for guest VMs—**In certain cases, operations are invoked by guest operating systems, instead of being executed directly by the host hardware, and they may have to be executed by the hypervisor because of their privileged nature.
   - **Management of VMs (also called VM life cycle management) —**This is about configuring guest VMs and controlling VM states (for example, start, pause, stop).
   - **Administration of hypervisor platform and hypervisor software—**This involves setting parameters for user interactions with the hypervisor host as well as hypervisor software.

6. There are two types of hypervisors based on the presence of the operating system between the hypervisor and the host. A type 1 hypervisor is loaded as a software layer directly onto a physical server; this is referred to as *native virtualization*. The type 1 hypervisor can directly control the physical resources of the host. A type 2 hypervisor exploits the resources and functions of a host operating system and runs as a software module on top of the operating system; this is referred to as *hosted virtualization*. It relies on the operating system to handle all the hardware interactions on the hypervisor's behalf.

7. In container virtualization, a software piece known as a *virtualization container* runs on top of the host operating system kernel and provides an isolated execution environment for applications. Unlike hypervisor-based VMs, containers do not aim to emulate physical servers. Instead, all containerized applications on a host share a common operating system kernel. This eliminates the need for resources to run a separate operating system for each application and can greatly reduce overhead. For containers, only a small container engine is required as support for the containers. The container engine sets up each container as an isolated instance by requesting dedicated resources from the operating system for each container. Each container app then directly uses the resources of the host operating system.

https://t.me/learningnets

8. The three categories of network storage systems are as follows:

   - **Direct attached storage (DAS)—**This is internal server hard drives that are generally captive to the attached server.
   - **Storage area network (SAN)—**A SAN is a dedicated network that provides access to various types of storage devices, including tape libraries, optical jukeboxes, and disk arrays. To servers and other devices in the network, a SAN's storage devices look like locally attached devices.
   - **Network attached storage (NAS)—**NAS systems are networked appliances that contain one or more hard drives that can be shared with multiple, heterogeneous computers. Their specialized role in networks is to store and serve files. NAS disk drives typically support built-in data protection mechanisms, including redundant storage containers or redundant arrays of independent disks (RAID). NAS enables file-serving responsibilities to be separated from other servers on the network and typically provides faster data access than traditional file servers.

9. A service level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider is obligated to meet. SLAs are output based, with the sole purpose of specifically defining what service the customer will receive. Companies that establish SLAs include IT service providers, managed service providers, and cloud computing service providers. Three important types of SLAs are as follows:

   - **Network provider SLA—**A network SLA is a contract between a network provider and a customer that defines specific aspects of the service that is to be provided.
   - **Computer security incident team SLA—**A computer security incident response team (CSIRT) SLA typically describes the response to an incident, preventive actions to stop such incidents, and steps takes to beef up security of the system.
   - **Cloud service provider SLA—**An SLA for a cloud service provider should include security guarantees such as data confidentiality, integrity guarantees, and availability guarantees for cloud services and data.

10. An organization can ensure effective backup by following these policies:

    - Backups of all records and software must be retained such that computer operating systems and applications are fully recoverable. The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
    - Tri level or, better, *N* level redundancy must be maintained at the server level.
    - At a minimum, one fully recoverable version of all data must be stored in a secure offsite location. An offsite location may be in a secure space in a separate building or with an approved offsite storage vendor.

https://t.me/learningnets

- Derived data should be backed up only if restoration is more efficient than re-creation in the event of failure.
- All data information accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. Data located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested on an annual basis.

11. FIPS 199 describes three types of sites for backup:
    - **Cold site—**This is a backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from the main computing location to an alternate site
    - **Warm site—**This is an environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.
    - **Hot site—**This constitutes a fully operational offsite data processing facility, equipped with hardware and software, with prime use in the event of an information system disruption.
12. The following are some useful guidelines for developing a change management strategy:
    - **Communication—**Adequate advance notice should be given, especially if a response is expected and a proper response matrix with contact details is known.
    - **Maintenance window—**A maintenance window is a defined period of time during which maintenance, such as patching software or upgrading hardware components, can be performed. Clearly defining a regular maintenance window can be advantageous as it provides a time when users should expect service disruptions
    - **Change committee—**The change committee reviews change requests and determine whether the changes should be made. In addition, it may determine that certain changes to the proposed plan for implementing the change must be made in order for it to be acceptable.

https://t.me/learningnets

- **Critical changes—**There must be provision to accommodate critical changes that are needed to be rushed into production, creating an unscheduled change.
- **Plan the change—**All aspects associated with the change (who what, when, and so on) must be carefully planned.
- **Document change requests—**A change request form provides detailed information about the change and is appropriate for changes affecting data classified as confidential (highest, most sensitive) where protection is required by law and where the asset risk is high and involves information that provides access to resources, physical or virtual.
- **Test the change—**The change should be tested prior to implementation.
- **Execute the change—**The change should be properly executed.
- **Keep a record of the change—**A log or other record of all changes should be kept to supplement the change request document.

Chapter 12

1. Key functions of network management are as follows:
   - **Fault management—**This refers to facilities that enable the detection, isolation, and correction of abnormal operation of the OSI environment.
   - **Accounting management—**This refers to facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects.
   - **Configuration management—**This refers to facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for continuous operation of interconnection services.
   - **Performance management—**This refers to facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities.
   - **Security management—**This refers to aspects of OSI security that are essential to operate OSI network management correctly and to protect managed objects.
2. Some of the key tasks performed by a network management entity or NME are as follows:
   1. Collect statistics on communications and network-related activities.
   2. Store of statistics locally.
   3. Respond to commands from the network control center, including commands to do the following:
      - Transmit collected statistics to the network control center
      - Change a parameter (example, a timer used in a transport protocol)

https://t.me/learningnets

- Provide status information (example, parameter values, active links)
- Generate artificial traffic to perform a test

4. Send messages to the NCC when local conditions undergo a significant change.

3. In a decentralized network management scheme, there may be multiple top-level management stations, called *management servers*. Each such server might directly manage a portion of the total pool of agents. However, for many of the agents, the management server delegates responsibility to an intermediate manager. The intermediate manager plays the role of manager to monitor and control the agents under its responsibility. It also plays an agent role in providing information and accepting control from a higher-level management server. This scheme reduces total network traffic and distributes the processing burden.

4. According to Cisco, the network management architecture has three layers:

   - **Element management layer—**This layer provides an interface to the network devices and communications links in order to monitor and control them. This layer captures events and fault occurrences through a combination of direct polling and unsolicited notification by network elements. Management function modules provide interfaces to specific elements, allowing elements from different manufacturers to be incorporated under a single management control.
   - **Network management layer—**This layer provides a level of abstraction that does not depend on the details of specific elements. In terms of event management, this layer takes input from multiple elements, correlates the information received from the various sources (also referred to as root-cause analysis), and identifies the event that has occurred.
   - **Service management layer—**The service management layer is responsible for adding intelligence and automation to filtered events, event correlation, and communication between databases and incident management systems.

5. Firewalls use four techniques to control access and enforce the site's security policy:

   - **Service control—**A firewall determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; it may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a web or mail service.
   - **Direction control—**A firewall determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
   - **User control—**A firewall controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as that provided by IPsec.

https://t.me/learningnets

- **Behavior control—**A firewall controls how particular services are used. For example, the firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local web server.

6. Principal types of firewalls are:
   - Packet filtering firewall
   - Stateful inspection firewalls
   - Application-level gateway
   - Circuit-level gateway
7. Packet filters have following weaknesses:
   - A packet filtering firewall cannot prevent attacks that employ application-specific vulnerabilities or functions as these firewalls do not examine upper-layer data. For example, if a packet filtering firewall cannot block specific application commands and if a packet filtering firewall allows a given application, all functions available within that application will be permitted.
   - The logging functionality present in packet filtering firewalls is limited as these firewalls have access to limited information.
   - Most packet filtering firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality.
   - Packet filtering firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filtering firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered.
   - Packet filtering firewalls are susceptible to security breaches caused by improper configurations. This means it is easy to accidentally configure a packet filtering firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.
8. Some of the important characteristics of automated network device configuration management tools are as follows:
   - **Multivendor device support—**The solution should support all device types from all popular vendors.
   - **Discovery capability for device addition—**The solution should have provision for discovering the devices in the network and automatically adding them, in addition to other device addition options.
   - **Communication protocols—**The solution should support a wide range of protocols to establish communication with the device and transfer configuration files.

https://t.me/learningnets

- **Secure storage—**The configuration data should be stored in encrypted form and protected against intrusion.
- **Inventory—**The solution should provide an informative inventory of the devices being managed. It should provide various details, such as serial numbers, interface details, chassis details, port configurations, IP addresses, and hardware properties of the devices.
- **Configuration operations and schedules—**The solution should provide simple, intuitive options in the GUI to carry out various configuration operations, such as configuration retrieval and viewing, editing, and uploading configurations back to the device.
- **Configuration versioning—**A version number should be associated with the configuration of each device and incremented with each change.
- **Baseline configuration—**The solution should have provision for labeling the trusted configuration version of each device as a baseline version to enable administrators to roll back configurations to the baseline version in the event of a network outage.
- **Access control—**An attribute-based or role-based access control scheme should be used to provide security when multiple users have access to configuration tools.
- **Approval mechanism—**The security policy in an enterprise may require certain types of changes carried out by certain levels of users to be reserved for review and approval by top administrators prior to the deployment of the changes.

9. A TIA-942 compliant data center has following functional areas:

- **Computer room—**This is the portion of the data center that houses date processing equipment.
- **Entrance room—**This area houses external network access provider equipment and provides an interface between the computer room equipment and the enterprise cabling systems.
- **Main distribution area—**This is a centrally located area that houses the main cross-connect as well as core routers and switches for LAN and SAN infrastructures.
- **Horizontal distribution area (HDA)—**The HDA serves as the distribution point for horizontal cabling and houses cross-connects and active equipment for distributing cable to the equipment distribution area.
- **Equipment distribution area (EDA)—**The EDA houses equipment cabinets and racks, with horizontal cables terminating with patch panels.
- **Zone distribution area (ZDA)—**This is an optional interconnection point in the horizontal cabling between the HDA and EDA. The ZDA can act as a consolidation point for reconfiguration flexibility or for housing freestanding equipment, such as mainframes.

https://t.me/learningnets

10. Some of the main risks associated with wireless access are as follows:

    - **Insufficient policies, training, and awareness—**Wireless security controls must include policies and user awareness training specifically for wireless access. These should include procedures regarding uses of wireless devices and an understanding of relevant risks.
    - **Access constraints—**Wireless access points repeatedly send out signals to announce themselves so that users can find them to initiate connectivity. This signal transmission occurs when beacon frames containing the access points' service set identifiers (SSIDs) are sent unencrypted. SSIDs are names or descriptions used to differentiate networks from one another. This signal transmission makes it easy for unauthorized users to learn the network name and attempt an attack or intrusion.
    - **Rogue access points—**Rogue access points are APs that users install without coordinating with IT. Access controls, encryption, and authentication procedures enable IT to maintain control.
    - **Traffic analysis and eavesdropping—**An eavesdropper can snoop the communication and interpret the communication. To counter this threat, it is necessary to use a strong user authentication technique and to encrypt all traffic.
    - **Insufficient network performance—**Poor performance may be due to an imbalance in the use of access points, insufficient capacity planning, or a denial-of-service (DoS) attack.
    - **Hacker attac**ks**—**Hackers attempt to gain unauthorized access over wireless networks. Intrusion detection systems, antivirus software, and firewalls are mitigation techniques.
    - **Physical security deficiencies—**This is in the domain of physical security. Both network devices and mobile devices should be subject to physical security policies and procedures.

11. SP 800-41 defines firewall planning and implementation phases in the following manner:

    1. **Plan—**The first phase of the process involves identifying all requirements for an organization to consider when determining what firewall to implement to enforce the organization's security policy.
    2. **Configure—**The second phase involves all facets of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system.
    3. **Test—**The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of testing are to evaluate the functionality, performance, scalability, and security of the solution and to identify any issues—such as interoperability—with components.
    4. **Deploy—**When testing is complete and all issues are resolved, the next phase focuses on deployment of the firewall into the enterprise.

https://t.me/learningnets

5. **Manage—**After the firewall has been deployed, it is managed throughout its life cycle, including component maintenance and support for operational issues. This life cycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

12. In general, email security threats can be classified as follows:

- **Authenticity-related threat—**This threat arises from not being able to verify authenticity. It could result in unauthorized access to an enterprises' email system. Another threat in this category is deception, in which the purported author isn't the actual author.
- **Integrity-related threat—**This threat could result in unauthorized modification of email content.
- **Confidentiality-related threat—**This threat could result in unauthorized disclosure of sensitive information.
- **Availability-related threat—**This threat could prevent end users from being able to send or receive email.

13. ISO 27002 advocates the following ways to protect email:

- Protecting messages from unauthorized access, modification, or denial of service commensurate with the classification scheme adopted by the organization.
- Ensuring correct addressing and transportation of the message.
- Ensuring reliability and availability of the service.
- Giving legal consideration, such as requirements for electronic signatures.
- Obtaining approval prior to using external public services such as instant messaging and social networking.
- Using file sharing instead of sending sensitive data unencrypted over email.
- Using stronger levels of authentication to control access from publicly accessible networks.

14. The two main types of infrastructure equipment that support VoIP are as follows:

- **IP PBX—**This is designed to support digital and analog phones and connect to IP-based networks using VoIP, as well as provide, if needed, a connection to the public switched telephone network using traditional technology.
- **Media gateway—**This connects different physical networks in order to provide end-to-end connectivity. An important type of media gateway connects a VoIP network to a circuit-switched telephone network, providing the necessary conversion and signaling.

https://t.me/learningnets

15. Some of the key threats for VoIP usage are as follows:

    - **Spam over Internet telephone (SPIT)—**Unsolicited bulk messages may be broadcast over VoIP to phones connected to the Internet. Although marketers already use voicemail for commercial messages, IP telephony makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately.
    - **Eavesdropping—**Interception of control packets enables an adversary to listen in on an unsecured VoIP call.
    - **Theft of service—**This type of attack involves capturing access codes, allowing the adversary to get into the VoIP provider network and then use the facility.
    - **Man-in-the middle attack—**This type of attack involves an adversary inserting as a relay point between two ends of a VoIP call. In addition to eavesdropping, the adversary could divert a call to a third party or generate simulated voice content to create misleading impressions or cause operational errors.

16. The Standards Customer Council defines the following key components of a cloud service agreement (CSA):

    - **Customer agreement—**This section describes the overall relationship between the customer and the provider. Its terms include how the customer is expected to use the service, methods of charging and paying, reasons a provider may suspend service, termination, and liability limitations.
    - **Acceptable use policy—**This section prohibits activities that providers consider to be improper or outright illegal uses of their service. Conversely, the provider usually agrees not to violate the intellectual property rights of the customer.
    - **Cloud service level agreements—**These agreements define a set of service level objectives. These objectives may concern availability, performance, security, and compliance/privacy. The SLA specifies thresholds and financial penalties associated with violations of these thresholds. Well-designed SLAs can significantly contribute to avoiding conflict and can facilitate the resolution of an issue before it escalates into a dispute.
    - **Privacy policies—**These policies describe the different types of information collected; how that information is used, disclosed, and shared; and how the provider protects that information.

Chapter 13

1. ICT, which stands for information communication technology, comprises a collection of devices, networking components, applications, and systems that together allow people and organizations to interact in the digital world. ICT is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

https://t.me/learningnets

2. A supply chain is an end-to-end network of all the individuals, organizations, resources, activities, and technology involved from the creation to the sale of a product or service. It typically starts from the delivery of source materials from the supplier to the manufacturer and goes through to eventual delivery to the end user. In this traditional use, the term applies to the entire chain of production and use of physical products. An ICT supply chain is a linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer.
3. Three types of flows are associated with a supply chain:
    - **Product/service flow—**This refers to the flow of intermediate products or services. A key requirement is a smooth flow of an item from the provider to the enterprise and then on to the internal user or external customer.
    - **Information flow—**This comprises the request for key information items such as quotations, purchase orders, monthly schedules, engineering change requests, quality complaints, and reports on supplier performance from the customer side to the supplier. From the producer's side to the consumer's side, the information flow consists of the presentation of the company, offer, confirmation of purchase order, reports on action taken on deviation, dispatch details, report on inventory, invoices, and so on.
    - **Money flow—**This refers to the actual flow of money or currency from client to seller. On the basis of the invoice raised by the producer, the clients examine the order for correctness. If the claims are correct, money flows from the clients to the respective producer. Flow of money is also observed from the producer side to the clients, in the form of debit notes.
4. Key elements of a supply chain management are as follows:
    - **Demand management—**This function meets all demands for goods and services to support the marketplace. It involves prioritizing demand when supply is lacking. Proper demand management facilitates the planning and use of resources for profitable business results.
    - **Supplier qualification—**This refers to ability to provide an appropriate level of confidence that suppliers, vendors, and contractors are able to supply consistent quality of materials, components, and services, in compliance with customer and regulatory requirements.
    - **Supplier negotiation—**This is a formal process of communication in which two or more people come together to seek mutual agreement over an issue(s). Negotiation is particularly appropriate when issues besides price are important for the buyer or when competitive bidding will not satisfy the buyer's requirements on those issues.

https://t.me/learningnets

- **Sourcing, procurement, and contract management—**Sourcing refers to the selection of a supplier(s). Procurement is the formal process of purchasing goods or services. Contract management is a strategic management discipline employed by both buyers and sellers whose objectives are to manage customer and supplier expectations and relationships, control risk and cost, and contribute to organizational profitability/success.
- **Logistics and inventory control—**Here logistics refers to the process of strategically managing the procurement, movement, and storage of materials, parts, and finished inventory (and the related information flows) through the organization and its marketing channels. Inventory control is the tracking and accounting of procured items.
- **Invoice, reconciliation, and payment—**This is about payment of goods and services.
- **Supplier performance monitoring—**This includes the methods and techniques used to collect information that can be used to measure, rate, or rank a supplier's commitment to honor commitments and enterprise objectives on a continuous basis.

5. According to SP 800-161, the three tiers of risk management model that are defined in SP 600-39 are as follows:
   - **Tier 1—**This tier is engaged in the development of the overall ICT SCRM strategy, determination of organization-level ICT SCRM risks, and setting of the organizationwide ICT SCRM policies to guide the organization's activities in establishing and maintaining organizationwide ICT SCRM capability
   - **Tier 2—**This tier is engaged in prioritizing the organization's mission and business functions, conducting mission-/business-level risk assessment, implementing Tier 1 strategy, establishing an overarching organizational capability to manage ICT supply chain risks, and guiding organizationwide ICT acquisitions and their corresponding SDLCs.
   - **Tier 3—**This tier is involved in specific ICT SCRM activities to be applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' SDLCs.
6. Key external risks of a supply chain are as follows:
   - **Demand—**This relates to potential or actual disturbances to the flow of product, information, and cash emanating from within the network between the focal firm and its market. For example, disruptions in the cash resource within the supply chain can have a major impact on the operating capability of organizations.
   - **Supply—**This is the upstream equivalent of demand risk; it relates to potential or actual disturbances to the flow of product or information emanating within the network upstream of the focal firm. The disruption of key resources coming into the organization can have a significant impact on the organization's ability to perform.
   - **Environmental—**This refers to the risk associated with external and, from the firm's perspective, uncontrollable events. The risks can impact the firm directly or through its

https://t.me/learningnets

suppliers and customers. Environmental risk is broader than just natural events such as earthquakes or storms. It also includes, for example, changes created by governing bodies such as changes in legislation or customs procedures, as well as changes in the competitive climate.

7. Key internal risks of a supply chain are as follows:

   - **Processes—**This refers to the sequences of value-adding and managerial activities undertaken by the firm. Process risk relates to disruptions to key business processes that enable the organization to operate. Some processes are key to maintaining the organization's competitive advantage, and others underpin the organization's activities.
   - **Control—**This refers to the assumptions, rules, systems, and procedures that govern how an organization exerts control over the processes and resources. In terms of the supply chain, this may be order quantities, batch sizes, safety stock policies, and so on, plus the policies and procedures that govern asset and transportation management.
   - **Mitigation—**This refers to a hedge against risk built in to the operations themselves. Mitigation needs to be considered during the supply chain design process; if it is not undertaken, the risk profile can be increased. Contingency is the existence of a prepared plan and the identification of resources that can be mobilized in the event of a risk being identified. This requires all stakeholders in the supply chain to understand what resources can be mobilized and the procedures to do this.

8. SP 800-161 organizes security controls for SCRM into the following categories:

   - Access control
   - Awareness and training
   - Audit and accountability
   - Security assessment and authorization
   - Configuration management
   - Contingency planning
   - Identification and authentication
   - Incident response
   - Maintenance
   - Media protection
   - Physical and environmental protection
   - Planning
   - Program management

https://t.me/learningnets

- Personnel security
- Provenance
- Risk assessment
- System and services acquisition
- System and communications protection
- System and information security

9. The three security controls of the provenance family are as follows:
   - **Provenance policy and procedures—**This provides guidance for implementing a provenance policy.
   - **Tracking provenance and developing a baseline—**This provides details concerning the tracking process.
   - **Auditing roles responsible for provenance—**This indicates the role auditing plays in an effective provenance policy.
10. Cloud computing is a model for enabling ubiquitous, convenient, on-demand, and scalable network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
11. The key characteristics of cloud computing are as follows:
    - **Broad network access—**This refers to wide network coverage over a range of devices. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, laptops, PDAs) as well as other traditional or cloud-based software services.
    - **Rapid elasticity—**This refers to the ability to expand and reduce resources according to specific service requirements. For example, there may be a need for large number of server resources for the duration of a specific task. After that task, those resources can be released.
    - **Measured service—**Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
    - **On-demand self-service—**By this tenant, a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Because the service is on demand, the resources are not permanent parts of the IT infrastructure.

https://t.me/learningnets

- **Resource pooling—**The provider's computing resources may be pooled to serve multiple consumers, using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

12. The three service models of cloud computing, according to NIST, are as follows:

    - **Software as a service (SaaS)—**In this model, the consumer can use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains these functions from the cloud service. SaaS eliminates the complexity of software installation, maintenance, upgrades, and patches. Examples of services at this level are Gmail, Google's email service, and Salesforce.com, which helps firms keep track of their customers.
    - **Platform as a service (PaaS)—**In this model, the consumer can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS often provides middleware-style services such as database and component services for use by applications.
    - **Infrastructure as a service (IaaS)—**In this model, the consumer is provided with processing, storage, network, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems in a short period of time.

13. NIST defines four deployment models:

    - **Public cloud—**Here the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The cloud provider is responsible for both the cloud infrastructure and the control of data and operations within the cloud.
    - **Private cloud—**Here the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises. The cloud provider is responsible only for the infrastructure and not for the control.
    - **Community cloud—**Here the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, compliance considerations). It may be managed by the organization or a third party and may exist on premises or off premises.
    - **Hybrid cloud—**Here the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by

https://t.me/learningnets

standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load balancing between clouds).

14. NIST's cloud computing reference architecture defines the following central elements:

- **Cloud consumer—**This refers to a person or an organization that maintains a business relationship with, and uses service from, cloud providers.
- **Cloud provider—**This refers to a person, an organization, or an entity responsible for making a service available to interested parties.
- **Cloud auditor—**This refers to a party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
- **Cloud broker—**This refers to an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.
- **Cloud carrier—**This refers to an intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.

15. Some of the threats to cloud service users are as follows:

- **Responsibility ambiguity—**This arises from the fact that cloud service users consume delivered resources through service models, thereby making the customer-built IT system dependent on those services. The lack of a clear definition of responsibility among cloud service users and providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomalies or incidents.
- **Loss of governance—**This refers to reduction on full control of IT systems. The decision by an enterprise to migrate a part of its own IT system to a cloud infrastructure implies giving partial control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS delegates only hardware and network management to the provider, while SaaS also delegates operating system, application, and service integration in order to provide a turnkey service to the cloud service user.
- **Loss of trust—**It is sometimes difficult for a cloud service user to recognize the provider's trust level due to the black-box feature of the cloud service. There is no measure to obtain and share the provider's security level in a formalized manner.
- **Service provider lock-in—**This refers to tight binding with the cloud service provider. Loss of governance could result in lack of freedom in how to replace one cloud provider with another. This could be the case if a cloud provider relies on nonstandard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.
- **Insecure cloud service user access—**As most of the resource deliveries are through remote connections, non-protected APIs (mostly management APIs and PaaS services)

https://t.me/learningnets

are among the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities may achieve results.

- **Lack of information/asset management—**Because the physical assets are not hosted at the user's premises, a cloud service user may have serious concerns about lack of information/asset management from cloud service providers, such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), and disaster recovery. Furthermore, cloud service users also may have important concerns about exposure of data to foreign governments and compliance with privacy laws.
- **Data loss and leakage—**This threat may be strongly related to the preceding item. However, loss of an encryption key or a privileged access code will bring serious problems to cloud service users. Accordingly, lack of cryptographic management information, such as encryption keys, authentication codes, and access privilege, will lead to sensitive damages, such as data loss and unexpected leakage to the outside.

16. The Standards Customer Council defines the following key components of a cloud service agreement (CSA):

- **Customer agreement—**This section describes the overall relationship between the customer and the provider. Its terms include how the customer is expected to use the service, methods of charging and paying, reasons a provider may suspend service, termination, and liability limitations.
- **Acceptable use policy—**This section prohibits activities that providers consider to be improper or outright illegal uses of their service. Conversely, the provider usually agrees not to violate the intellectual property rights of the customer.
- **Cloud service level agreements—**These agreements define a set of service level objectives. These objectives may concern availability, performance, security, and compliance/privacy. The SLA specifies thresholds and financial penalties associated with violations of these thresholds. Well-designed SLAs can significantly contribute to avoiding conflict and can facilitate the resolution of an issue before it escalates into a dispute.
- **Privacy policies—**These policies describe the different types of information collected; how that information is used, disclosed, and shared; and how the provider protects that information.

Chapter 14

1. Technical security controls are safeguards or countermeasures designed for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system (for example, biometric controls).

https://t.me/learningnets

2. Security architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. Its key characteristics are as follows:
   - It consists of a transparent and coherent overview of models, principles, starting points, and conditions that give a concrete interpretation of the information security policy, usually without speaking in terms of specific solutions.
   - It reduces a complex problem into models, principles and subproblems that can be understood.
   - The models and principles show where to take which type of measures, when the principles are applicable, and how the principles connect with other principles.
3. The SABSA model consists of six layers:
   1. **Contextual security architecture—**This layer describes the key business issues, starting with the assets, the motivation for providing security, the business processes, the organization, geographical dispersion, and key time-related considerations in these processes.
   2. **Conceptual security architecture—**This layer considers the security characteristics of each of the business drivers. The SABSA ICT Business Attribute Taxonomy, a set of attributes described in business language that reflect security characteristics, has been developed for this. The standard taxonomy has 50 attributes in addition to the traditional security attributes confidentiality, availability, and integrity. By associating a set of attributes with each business driver, it is possible to define a security architecture in a way that provides full traceability to business needs.
   3. **Logical security architecture—**This layer provides a design layer view, focusing on the delivery of services and information to meet the security concept.
   4. **Physical security architecture—**This layer takes care of the delivery of tangible items to support the logical services.
   5. **Component security architecture—**This layer defines the hardware and tools to deliver the physical design and provides a mapping to conform to standards.
   6. **Security service management architecture—**This layer takes care of issues related to how the organization manages the architecture
4. The two-way traceability is as follows:
   - **Completeness—**Completeness answers the question "Has every business requirement been met?" The layers and matrix allow you to trace every requirement through to the components that provide a solution.
   - **Justification—**Justification answers the question "Is every component of the architecture needed?" When someone questions "Why are we doing it this way?" the rationale is plain if you trace back to the business requirements that drive the specific solution.

https://t.me/learningnets

5. Some common types of malware are as follows:
    - Adware
    - Auto-rooter
    - Backdoor/trapdoor
    - Exploit
    - Downloader
    - Dropper
    - Flooder
    - Keylogger
    - Kit (virus generator)
    - Logic bomb
    - Malware as a Service
    - Mobile code
    - Potentially unwanted program (PUP)
    - Ransomware
    - Remote access Trojan or RAT
    - Rootkit
    - Spammer program
    - Spyware
    - Trojan horse
    - Virus
    - Web drive-by
    - Work
    - Zombie/bot
6. SP 800-83 indicates that good malware software has the following capabilities:
    - It must scan critical host components, such as startup files and boot records.
    - It must watch real-time activities. Good anti-malware software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as on-access scanning.

https://t.me/learningnets

- It must monitor common applications, such as email, instant messaging software, email clients, and Internet browsers. Good anti-malware software monitors activity involving the applications most likely to be used to infect hosts or spread malware to other hosts.
- It must scan each file for known malware. Anti-malware software on hosts should be configured to scan all hard drives regularly to identify any file system infections and, optionally, depending on organization security needs, to scan removable media inserted into the host before allowing its use.
- It must be capable of identifying common types of malware as well as attacker tools.
- It must be capable of disinfecting and quarantining files. Disinfecting files refers to removing malware from within a file, and quarantining files means storing files containing malware in isolation for future disinfection or examination.

7. Identity and access management (IAM) is a framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management. Typically, these policies fall into two categories:

   - **Provisioning process—**Provides users with the accounts and access rights they require to access systems and applications
   - **User access process—**Manages the actions performed each time a user attempts to access a new system, such as authentication and sign-on

   There are three ways to deploy it:

   - **Centralized—**All access decisions, provisioning, management, and technology are concentrated in a single physical or virtual location. Policies, standards, and operations are pushed out from this single location.
   - **Decentralized—**Local, regional, or business units make the decisions for all access choices, provisioning, management, and technology.
   - **Federated—**Each organization subscribes to a common set of policies, standards, and procedures for the provisioning and management of users. Alternatively, the organizations can buy a service from a supplier.

8. Some of the best practices for avoiding common security mistakes with IAM are as follows:

   - Proactively train staff to spot warning signs of phishing attacks and social engineering.
   - Patch promptly to guard against attacks.
   - Sensibly encrypt data.
   - Deploy multifactor authentication judiciously.
   - Implement least-privilege access controls by giving access to systems only when it is needed.

https://t.me/learningnets

- Implement controls and monitoring tools to access privileged systems and data.
- Protect your mobile and cloud applications.
- Stop breaches that start on endpoints by granting access to apps and infrastructure from trusted and secured endpoints.
- Implement portals for accessing the web as SaaS applications using single sign-on (SSO).

9. An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Typically, it detects and reports all types of anomalies. There are two types of IDSs:
   - **Host-based IDS—**This monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Host-based IDSs can determine exactly which processes and user accounts are involved in a particular attack on the operating system.
   - **Network-based IDS—**This monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.
10. Two generic approaches to intrusion detection are as follows:
    - **Misuse detection—**Misuse detection is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents. Misuse detectors use various pattern-matching algorithms, operating on large databases of attack patterns, or signatures. An advantage of misuse detection is that it is accurate and generates few false alarms. A disadvantage it that it cannot detect novel or unknown attacks.
    - **Anomaly detection—**Anomaly detection is based on detection of activity that is different from the normal behavior of system entities and system resources. An advantage of anomaly detection is that it is able to detect previously unknown attacks based on an audit of activity. A disadvantage is that there is a significant trade-off between false positives and false negatives.
11. Some common ways to recognize sensitive data in real time are as follows:
    - **Rule-based—**Regular expressions, keywords, and other basic pattern-matching techniques are best suited for basic structured data, such as credit card numbers and Social Security numbers. This technique efficiently identifies data blocks, files, database records, and so on that contain easily recognized sensitive data.
    - **Database fingerprinting—**This technique searches for exact matches to data loaded from a database, which can include multiple-field combinations, such as name, credit card number, and CVV number.

https://t.me/learningnets

- **Exact file matching—**This technique involves computing the hash value of a file and monitoring for any files that match that exact fingerprint. This is easy to implement and can be used to check whether a file has been accidentally stored or transmitted in an unauthorized manner.
- **Partial document matching—**This technique looks for a partial match on a protected document. It involves the use of multiple hashes on portions of the document, such that if a portion of the document is extracted and filed elsewhere or pasted into an email, it can be detected.

12. Principal users of DRM system are as follows:
    - **Content provider—**The content provider holds digital rights to the content and wants to protect these rights (for example, a music record label, a movie studio).
    - **Distributor—**The distributor provides distribution channels, such as an online shop or a web retailer. For example, an online distributor receives the digital content from the content provider and creates a web catalog that presents the content and rights metadata for the content promotion (for example, IndiaCast).
    - **Consumer—**The consumer uses the system to access the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license (for example, Netflix users).
    - **Clearinghouse—**The clearinghouse handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly (for example, PCH/Media).
13. Cryptography is a method of converting ordinary plaintext into unintelligible text and vice versa. It is a way of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication. It is useful in the following processes:
    - **Data encryption—**Data encryption is a powerful and cost-effective means of providing data confidentiality and data integrity. Once data are encrypted, the ciphertext does not have to be protected against disclosure. Further, if ciphertext is modified, it does not decrypt correctly.
    - **Data integrity—**Data integrity is established by cryptographic algorithms that can provide an effective way to determine whether a block of data (for example, email text, message, file, database record) has been altered in an unauthorized manner.
    - **Data signature—**The digital signature, or electronic signature, is the electronic equivalent of a written signature that can be recognized as having the same legal status as a written signature. Furthermore, digital signature algorithms can provide a means of linking a document with a particular person, as is done with a written signature.

https://t.me/learningnets

- **User authentication—**Cryptography is a powerful authentication tool. Instead of communicating passwords over an open network, authentication can be performed by demonstrating knowledge of a cryptographic key. A one-time password, which is not susceptible to eavesdropping, can be used.

14. Symmetric encryption has the following five ingredients:

    - **Plaintext—**This refers to the original message or data block that is fed into the algorithm as input.
    - **Encryption algorithm—**This performs various substitutions and transformations on the plaintext.
    - **Secret key—**This is one of the main inputs to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
    - **Ciphertext—**This refers to the scrambled message produced as output. It depends on the plaintext and the secret key. For a given data block, two different keys produce two different ciphertexts.
    - **Decryption algorithm—**This is the inverse of the encryption algorithm: It uses the ciphertext and the secret key and produces the original plaintext.

15. A public key encryption scheme has following ingredients:

    - **Plaintext—**This is the readable message or data block that is fed into the algorithm as input.
    - **Encryption algorithm—**This performs various transformations (mainly mathematical operations) on the plaintext.
    - **Public and private key—**This refers to a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.
    - **Ciphertext—**This refers to the scrambled message produced as output. It depends on the plaintext and the secret key. For a given data block, two different keys will produce two different ciphertexts.
    - **Decryption algorithm—**This is inverse of the encryption algorithm: It accepts the ciphertext and the matching key and produces the original plaintext.

16. SP 800-57 classifies key types as follows:

    - **Private and public signature keys—**An asymmetric key pair is used to generate and verify digital signatures.
    - **Symmetric authentication key—**This key is used for message authentication.
    - **Private and public authentication keys—**These keys are used to provide assurance of the identity of an originating entity (that is, source authentication) when establishing an authenticated communication session.

https://t.me/learningnets

- **Symmetric data encryption key—**This key is used to provide data confidentiality by encryption/decryption.
- **Symmetric key-wrapping key—**This key, also called a key-encryption key, is used to encrypt/decrypt other keys.
- **Symmetric random number generation key—**This key is used with a random number generation algorithm.
- **Symmetric master key—**This key is used to derive other symmetric keys (for example, data-encryption keys or key-wrapping keys) using symmetric cryptographic methods.
- **Private and public key-transport keys—**These keys are used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Symmetric key-agreement key—**This key is used to establish keys (for example, key wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors) using a symmetric key-agreement algorithm.
- **Private and public static key-agreement key—**This is a long-term key pair used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Private and public ephemeral key-agreement key—**This short-term key pair is used only once to establish one or more keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (example, initialization vectors).
- **Symmetric authorization key—**This key is used to provide privileges to an entity. The authorization key is known by the entity responsible for monitoring and granting access privileges for authorized entities and by the entity seeking access to resources.
- **Private and public authorization key—**This key is used to provide and verify privileges.

17. You should not use a key for a prolonged period of time because it becomes vulnerable to the following types of error:

- **Brute-force attacks—**With the increase in raw processing power and parallel computing, a given key length becomes increasingly vulnerable, and longer key lengths are advised. Any shorter keys still in use need to be retired as quickly as possible and longer key lengths employed.
- **Cryptanalysis—**Over time, flaws discovered in a cryptographic algorithm make it feasible to "break" the algorithm. An example of this is the original NIST standard hash algorithm, SHA-1, which was used in Digital Signature Algorithm. Once the weaknesses were discovered, NIST migrated to SHA-2 and SHA-3.

https://t.me/learningnets

- **Other security threats—**There are direct as well as indirect methods of attack. This includes attacks on the mechanisms and protocols associated with the keys, key modification, and achieving unauthorized disclosure. The longer a particular key is used for encryption and decryption, the greater the chance that some means of learning the key will succeed.

18. A public key certificate is a set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, called a certification authority, thereby binding the public key to the entity. Public key certificates are designed to provide a solution to the problem of public key distribution.

19. Common architectural components of a PKI system are as follows:

    - **End entity—**This refers to an end user; a device, such as a router or server; a process; or any other item that can be identified in the subject name of a public key certificate.
    - **Certification authority (CA)—**This refers to an authority trusted by one or more users to create and assign public key certificates. Optionally the certification authority may create the subjects' keys. CAs digitally sign public key certificates, which effectively binds the subject name to the public key.
    - **Registration authority—**This optional component can be used to offload many of the administrative functions that a CA ordinarily assumes. The RA is normally associated with the end entity registration process.
    - **Repository—**This denotes any method for storing and retrieving PKI-related information, such as public key certificates and CRLs. A repository can be an X.500-based directory with client access via Lightweight Directory Access Protocol (LDAP).
    - **Relying party—**This refers to any user or agent that relies on the data in a certificate in making decisions.

Chapter 15

1. A technical vulnerability is a hardware, software, or firmware weakness or design deficiency that leaves an information system open to assault, harm, or unauthorized exploitation, either externally or internally, thereby resulting in unacceptable risk of information compromise, information alteration, or service denial. Five key steps are involved in vulnerability management:

    1. **Plan vulnerability management—**This first step in managing technical vulnerabilities involves many things, such as integration with asset inventory, establishment of clear authority to review vulnerabilities, proper risk and process integration, and integration of vulnerabilities with the application/system life cycle.

https://t.me/learningnets

2. **Discover known vulnerabilities—**This involves monitoring sources of information about known vulnerabilities to hardware, software, and network equipment.
3. **Scan for vulnerabilities—**Apart from regular monitoring, enterprises should regularly scan software, systems, and networks for vulnerabilities and proactively address those that are found.
4. **Log and report—**After the vulnerability scan, the results should be logged to verify the activity of the regular vulnerability scanning tools.
5. **Remediate vulnerabilities—**The enterprise should deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. As a good practice, patches should be applied to all systems.

2. Key sources that are used to discover vulnerabilities are as follows:

   - **National Vulnerability Database (NVDB)** is a comprehensive list of known technical vulnerabilities in systems, hardware, and software.
   - **Computer emergency response team (CERT) or computer emergency readiness team—**Such a team is a cooperative venture that collects information about system vulnerabilities and disseminates it to systems managers. Hackers also routinely read CERT reports. Thus, it is important for system administrators to quickly verify and apply software patches to discovered vulnerabilities. One of the most useful of these teams is the U.S. Computer Emergency Readiness Team, which is a partnership between the Department of Homeland Security and the public and private sectors, intended to coordinate responses to security threats from the Internet. Another excellent resource is the CERT Coordination Center, which grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency.
   - **Packet Storm—**Packet Storm provides around-the-clock information and tools to help mitigate both personal data and fiscal loss on a global scale.
   - **SecurityFocus—**This site maintains two important resources: BugTraq and the SecurityFocus Vulnerability Database. BugTraq is a high-volume, full-disclosure mailing list for detailed discussion and announcement of computer security vulnerabilities. The SecurityFocus Vulnerability Database provides security professionals with up-to-date information on vulnerabilities for all platforms and services.
   - **Internet Storm Center (ISC)—**The ISC (maintained by the SANS Institute) provides a free analysis and warning service to thousands of Internet users and organizations and is actively working with Internet service providers to fight back against the most malicious attackers.

https://t.me/learningnets

3. An enterprise needs to address two challenges involved in scanning:
   - **Disruptions caused by scanning—**The scanning process can impact performance. IT operations staff need to be in the loop. They should be made aware of the importance and relevance of scans. Also, timing needs to be resolved to ensure that scanning does not conflict with regular maintenance schedules.
   - **Huge amounts of data and numerous false positives—**Technical vulnerability management practices can produce very large data sets. It is important to realize that even though a tool indicates that a vulnerability is present, frequently follow-up evaluations are needed validate these findings.
4. Three types of patch management techniques are commonly used:
   - **Agent-based scanning—**Requires an agent to be running on each host to be patched, with one or more servers managing the patching process and coordinating with the agents. Each agent is responsible for determining what vulnerable software is installed on the host, communicating with the patch management servers, determining what new patches are available for the host, installing those patches, and executing any state changes needed to make the patches take effect.
   - **Agent-less scanning—**Uses one or more servers that perform network scanning of each host to be patched and determine what patches each host needs. Generally, agentless scanning requires that servers have administrative privileges on each host so that they can return more accurate scanning results and so they have the ability to install patches and implement state changes on the hosts.
   - **Passive network monitoring—**Monitors local network traffic to identify applications (and, in some cases, operating systems) that are in need of patching. Unlike the other techniques, this technique identifies vulnerabilities on hosts that don't permit direct administrator access to the operating system, such as some Internet of Things (IoT) devices and other appliances.
5. A security event is any occurrence during which private company data or records may have been exposed. If a security event was proven to have resulted in a data or privacy breach, that event is deemed a security incident. For example, a delay in patching a security weakness in vital company software would be an event. It would only be deemed an incident after the security monitoring team confirms a resulting data breach by hackers who capitalized on the weakness.
6. You should log the following events:
   - **Operating system logs—**This includes successful user logon/logoff; failed user logon; user account change or deletion; service failure; password changes; service started or stopped; and object access denied.

https://t.me/learningnets

- **Network device logs—**These logs comprise traffic allowed through firewall, traffic blocked by firewalls, bytes transferred, protocol usage, detected attack activity, user account changes, and administrator access.
- **Web servers—**This is about excessive access attempts to nonexistent files, code (SQL, HTML) seen as part of the URL, attempted access to extensions not implement on the server, web service stopped/started/failed messages, failed user authentication; invalid request, and internal server errors.

7. You can do the following analysis on cleaned SEM data:
   - **Pattern matching—**You can look for data patterns within the fields of stored event records. A collection of events with a given pattern may signal a security incident.
   - **Scan detection—**Attacks often begins with scans of IT resources by the attacker, such as port scans, vulnerability scans, or other types of pings. If a substantial number of scans are found from a single source or a small number of sources, this may signal a security incident.
   - **Threshold detection—**You can detect threshold crossing. For example, if the number of occurrences of a type of event exceeds a given threshold in a certain time period, that can constitute an incident.
   - **Event correlation—**Correlation consists of using multiple events from a number of sources to infer that an attack or suspicious activity has occurred. For example, if a particular type of attack proceeds in multiple stages, the separate events that record those multiple activities need to be correlated in order to see the attack. Another aspect of correlation is to correlate particular events with known system vulnerabilities, which results in a high-priority incident.
8. You can categorize threat sources in following manner:
   - **Adversarial—**This type of threat comes from individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.
   - **Accidental—**This type of threat is spawned by erroneous actions taken by individuals in the course of executing their everyday responsibilities.
   - **Structural—**This type of threat originates from failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters.
   - **Environmental—**This type of threat arises from natural disasters and failures of critical infrastructures on which the organization depends but that are outside the control of the organization.
9. An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT

https://t.me/learningnets

attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry. A typical APT attack has the following pattern:

1. Conduct background research to find potential targets
2. Execute the initial attack on the chosen target(s)
3. Establish a foothold in the target environment
4. Enable persistent command and control over compromised computers in the target environment
5. Conduct enterprise reconnaissance to find the servers or storage facilities holding the targeted information
6. Move laterally to new systems to explore their contents and understand to what new parts of the enterprise can be accessed from the new systems
7. Escalate privileges from local user to local administrator to higher levels of privilege in the environment
8. Gather and encrypt data of interest
9. Exfiltrate data from victim systems
10. Maintain persistent presence

10. A variety of technical tools can be used to prevent delivery, such as the following:

- **Antivirus software (AVS)—**AVS is a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. Continuously running AVS can identify, trap, and destroy incoming known viruses. If a virus is detected, the AVS can be configured to trigger a scan of the rest of the IT infrastructure for indicators of compromise associated with this outbreak.
- **Firewall—**A firewall can block delivery attempts from known or suspected hostile sources.
- **Web application firewall (WAF)—**A WAF is a firewall that monitors, filters, or blocks data packets as they travel to and from a web application.
- **Intrusion prevention system (IPS)—**An IPS is a system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. This is similar to an intrusion detection system but is proactive in attempting to block the intrusion

11. You can counteract exploits by adopting following methods:

- **Host-based intrusion detection system (HIDS)—**When the exploit is inside the enterprise network and attacking hosts, a HIDS can detect and alert on such an attempt.
- **Regular patching—**Patching discovered vulnerabilities can contain the damage.
- **Data restoration from backups—**After an exploit is discovered and removed, it may be necessary to restore a valid copy of data from a backup.

https://t.me/learningnets

12. ISO 27035-1 lists the following objectives for security incident management:

    - Information security events are detected and dealt with efficiently. This involves deciding when they should be classified as information security incidents.
    - Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
    - The adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response.
    - A link with relevant elements from crisis management and business continuity management through an escalation process is established.
    - Information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents.
    - Lessons are learned quickly from information security incidents, vulnerabilities, and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

13. Key capabilities of a typical SIEM are as follows:

    - **Data aggregation—**The aggregator serves as a consolidating resource before data is sent to be correlated or retained.
    - **Data normalization—**This is the process of resolving different representations of the same types of data into a similar format in a common database.
    - **Correlation—**Event correlation is the function of linking multiple security events or alerts, typically within a given time window and across multiple systems, to identify anomalous activity that would not be evident from any singular event.
    - **Alerting—**After data that trigger certain responses, such as alerts or potential security problems, are gathered or identified, SIEM tools can activate certain protocols to alert users, such as notifications sent to the dashboard, an automated email, or a text message.
    - **Reporting/compliance—**Protocols in a SIEM can be established to automatically collect data necessary for compliance with company, organizational, and government policies. Both custom reporting and report templates (generally for common regulations such as Payment Card Industry Data Security Standards [PCI DSS] and the U.S. Sarbanes-Oxley Act) are typically part of a SIEM solution.
    - **Forensics—**This is the ability to search log and alert data for indicators of malicious or otherwise anomalous activities is the forensic function of the SIEM. Forensics, which is supported by the event correlation and normalization processes, requires highly customizable and detailed query capabilities and drill-down access to raw log files and archival data.

https://t.me/learningnets

- **Retention—**This refers to storing data for long periods so that decisions can be made based on more complete data sets.
- **Dashboards—**This refers to the primary interface to analyze and visualize data in an attempt to recognize patterns or target activity or data that does not fit into a normal pattern.

14. ISO 27035 classifies security incidents in the following way:
    - **Emergency—**Severe impact. These are incidents that:
        - Act on especially important information systems and
        - Result in especially serious business loss or
        - Lead to especially important social impact
    - **Critical—**Medium impact. These are incidents that:
        - Act on especially important information systems or important information systems and
        - Result in serious business loss or
        - Lead to important social impact
    - **Warning—**Low impact. These are incidents that:
        - Act on especially important information systems or ordinary information systems and
        - Result in considerable business loss or
        - Lead to considerable social impact
    - **Information—**No impact. These are incidents that:
        - Act on ordinary information systems and
        - Result in minor business loss or no business loss or
        - Lead to minor social impact or no social impact
15. Typical phases in a digital forensics process are as follows:
    1. **Preparation—**This refers to the planning and policy-making activities related to forensic investigation. SP 800-86 recommends the following considerations:
        - Organizations should ensure that their policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures.
        - Organizations should create and maintain procedures and guidelines for performing forensic tasks, based on the organization's policies and all applicable laws and regulations.

https://t.me/learningnets

- Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools. Organizations should ensure that their IT professionals are prepared to participate in forensic activities.

2. **Identification—**This phase is initiated when there is a request for a forensic analysis. This phase involves understanding the purpose of the request and the scope of the investigation, such as type of case, subjects involved, and system involved. The identification phase determines where the data of interest are stored and what data can be recovered and retrieved.
3. **Collection—**When the location or locations of data are identified, the forensic process ensures that the data are collected in a manner that preserves the integrity of the evidence.
4. **Preservation—**Several actions comprise the preservation of data process, including the following:
   - Creating a log that documents when, from where, how, and by whom data were collected
   - Storing the data in a secure fashion to prevent tampering or contamination
   - Logging each access to the data made for forensic analysis
5. **Analysis—**Examples of analysis tasks include:
   - Checking for changes to the system such as new programs, files, services, and users
   - Looking at running processes and open ports for anomalous behavior
   - Checking for Trojan horse programs and toolkits
   - Checking for other malware
   - Looking for illegal content
   - Looking for indicators of compromise
   - Determining the who, when, where, what, and how details of a security incident
6. **Reporting—**This phase involves publishing a report resulting from a forensic investigation. SP 800-86 lists the following factors that affect reporting for any type of investigation.
   - **Alternative explanations:** The available information may not provide a definitive explanation of the cause and nature of an incident. The analyst should present the best possible conclusions and highlight alternative explanations.
   - **Audience consideration:** An incident requiring law enforcement involvement requires highly detailed reports of all information gathered and can also require copies of all evidentiary data obtained. A system administrator might want to see network traffic and related statistics in great detail. Senior management might simply want a high-level overview of what happened, such as a simplified visual representation of how the attack occurred and what should be done to prevent similar incidents.

https://t.me/learningnets

- **Actionable information:** Reporting also includes identifying actionable information gained from data that allows an analyst to collect new sources of information. For example, a list of contacts may be developed from the data that can lead to additional information about an incident or a crime. Also, information that is obtained might help prevent future events, such as learning about a backdoor on a system that is to be used for future attacks, a crime that is being planned, a worm scheduled to start spreading at a certain time, or a vulnerability that could be exploited.

Chapter 16

1. Key elements of a security profile are as follows:
   - **Individuals—**Each local environment should have one or more staff members with specific information security responsibilities, as discussed subsequently. The profile should detail the types of users at the location, in terms of their application and data usage, level of security awareness training, security privileges, and whether they use mobile devices and, if so, what type.
   - **Business processes and information—**This area includes the types of information used and whether any sensitive information is accessible. The profile should include descriptions of business processes that involve user information access, as well as descriptions of any external suppliers (for example, cloud service providers).
   - **Technology use—**The profile should provide a description of the location housing the users and equipment. The profile should indicate to what degree the location is accessible to the public or to others who are not part of the organization, whether the physical space is shared with other organizations (for example, an office building or park), and any particular environmental hazards (for example, tornado zone).
2. Key responsibilities of a security coordinator are as follows:
   - Develop the local environment profile.
   - Determine the best way to implement enterprise security policy in the local environment.
   - Provide oversight of implementation of information security policy in the local environment.
   - Ensure that physical security arrangements are in place and adequate.
   - Assist with communicating security policies and requirements to local end users and local management.
   - Keep enterprise security executives and management informed of security-related developments.

https://t.me/learningnets

- Oversee or coordinate end-user awareness training.
- Coordinate area response to information security risk assessments.
- Coordinate area response to information security risk audit requests as directed.
- Ensure completion and submission of required documentation.

3. The following infrastructure items demand a high level of physical security:
   - **Information system hardware—**This includes data processing and storage equipment, transmission and networking facilities, and offline storage media, as well as supporting documentation.
   - **Physical facility—**This includes buildings and other structures housing the system and network components.
   - **Supporting facilities—**These facilities underpin the operation of the information system. This category includes electrical power, communication services, and environmental controls (heat, humidity, and so on).
   - **Personnel—**This refers to humans involved in the control, maintenance, and use of the information systems.
4. Key environmental threats to physical security are as follows:
   - **Natural disasters—**These are the source of a wide range of environmental threats to data centers, other information processing facilities, and personnel. These are potentially the most catastrophic of physical threats.
   - **Inappropriate temperature/humidity—**Computers and related equipment are designed to operate within a certain temperature range. Most computer systems should be kept between 10 and 32 degrees Celsius (between 50 and 90 degrees Fahrenheit). Outside this range, resources might continue to operate but may produce undesirable results. If the ambient temperature around a computer gets too high, the computer cannot adequately cool itself, and internal components can be damaged.
   - **Fire and smoke—**Fire is a serious threat to human life and property. The threat is not only from direct flame but may also come from heat, release of toxic fumes, water damage from fire suppression, and smoke damage.
   - **Water—**Water and other stored liquids in proximity to computer equipment pose an obvious threat of electrical short-circuit and subsequent fire. Moving water—such as in plumbing and weather-created water from rain, snow, and ice—also poses threats. Another common and catastrophic threat is floodwater.
   - **Chemical, radiological, and biological hazards—**Chemical, radiological, and biological hazards pose a growing threat, both from intentional attack and from accidental discharge. In general, the primary risk of these hazards is to human life. Radiation and chemical agents can also cause damage to electronic equipment.

https://t.me/learningnets

- **Dust—**Dust is a prevalent threat that is often overlooked. Even fibers from fabric and paper are abrasive and mildly conductive, although generally equipment is resistant to such contaminants. Larger influxes of dust can result from a number of incidents, such as a controlled explosion of a nearby building and a windstorm carrying debris from a wildfire. A more likely source of influx comes from dust surges that originate within the building due to construction or maintenance work.
- **Infestation—**This covers damage from a broad range of living organisms, including mold, insects, and rodents. High-humidity conditions can lead to the growth of mold and mildew, which can be harmful to both personnel and equipment. Insects, particularly those that attack wood and paper, are also a common threat.

5. Power utility problems can be broadly grouped into three categories:
   - **Undervoltage and power outages—**Undervoltage events range from temporary dips in the voltage supply, to brownouts (prolonged undervoltage), to power outages.
   - **Overvoltage—**Overvoltage is bigger threat than undervoltage. A surge of voltage can be caused by a utility company supply anomaly, by some internal (to the building) wiring fault, or by lightning. Damage is a function of intensity and duration, as well as the effectiveness of any surge protectors between IT equipment and the source of the surge.
   - **Noise—**Power lines can also be a conduit for noise. In many cases, spurious signals can endure through the filtering circuitry of the power supply and interfere with signals inside electronic devices, causing logical errors.

   Noise along a power supply line causes electromagnetic interference (EMI). This noise can be transmitted through space as well as through nearby power lines. Another source of EMI is high-intensity emissions from nearby commercial radio stations and microwave relay antennas. Even low-intensity devices, such as cellular telephones, can interfere with sensitive electronic equipment.

6. The following are some of the human-caused physical threats:
   - **Unauthorized physical access—**Information assets such as servers, mainframe computers, network equipment, and storage networks are generally located in a restricted area, with access limited to a small number of employees. Unauthorized physical access can lead to other threats, such as theft, vandalism, or misuse.
   - **Theft—**This threat includes theft of equipment and theft of data by copying. Eavesdropping and wiretapping also fall into this category. Theft can be at the hands of an outsider who has gained unauthorized access or by an insider.
   - **Vandalism—**This threat includes destruction of equipment and data.

7. Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multilayered defense system than to penetrate a single barrier.

https://t.me/learningnets

Defense in depth is appropriate and effective for physical security. The protective measures could include fences, gates, locked doors, electronic access (such as via smart card), armed guards, surveillance systems, and more. An appropriate first step is drawing a map of the physical facility and identifying the areas and entry points that need different rules of access or levels of security. These areas might have concentric boundaries, such as site perimeter, building perimeter, computer area, computer rooms, and equipment racks. There may also be side-by-side boundaries, such as visitor area, offices, and utility rooms. For concentric boundaries, physical security that provides access control and monitoring at each boundary provides defense in depth.

8. Important measures that are effective in addressing technical threats are as follows:

   - **Brief power interruptions—**It is advised to use an uninterruptible power supply (UPS) for each piece of critical equipment. A UPS is a battery backup unit that can maintain power to processors, monitors, and other equipment for a period of minutes. UPS units can also function as surge protectors, power noise filters, and automatic shutdown devices when the battery runs low.
   - **Longer blackouts or brownouts—**It is advisable to connect critical equipment to an emergency power source, such as a generator. For reliable service, management needs to address a range of issues, including product selection, generator placement, personnel training, and testing and maintenance schedules.
   - **Electromagnetic interference—**The organization should use a combination of filters and shielding. The specific technical details depend on the infrastructure design and the anticipated sources and nature of the interference.

9. An organization can counter human-caused physical threats by adopting following measures:

   - **Unauthorized physical access—**Physical access should be strictly on a need basis. Preventive measures include using locks and other hardware, card entry system, and proximity/touch access systems. Deterrence and response measures include intrusion alarms, sensors, and surveillance systems.
   - **Theft—**The measures to counter unauthorized physical access apply to the threat of theft as well. In addition, an organization should secure objects from being moved by bolting them down. For movable objects, an organization can incorporate a tracking device and provide an automated barrier that triggers an alarm when tagged objects cross the barrier.
   - **Vandalism—**Vandalism may involve environmental threats such as fire or technical threats such as interrupting or surging power, and the corresponding countermeasures apply.

https://t.me/learningnets

10. The SGP divides the local environment management category into two areas and five topics. These are the areas:
    - **Local environments—**This area deals with security issues in end-user environments and other local environments. It is subdivided into local environment profile and local security coordination topics.
    - **Physical and environmental security—**This area deals with the security of critical facilities against targeted cyber attack, unauthorized physical access, accidental damage, loss of power, fire, and other environmental or natural hazards. It is subdivided into three categories: physical protection, power supplies, and hazard protection.

Chapter 17

1. Business continuity is the ability of an organization to maintain essential functions during and after a disaster has occurred. Business continuity includes three key elements:
    - **Resilience—**Critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions (for example, through the use of redundancy and spare capacity).
    - **Recovery—**Arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.
    - **Contingency—**The organization must establish a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen.
2. Natural disasters threats that hamper business continuity are as follows:
    - **Accidental fire—**Sources include wildfires, lightning, wastebasket fires, and short-circuits.
    - **Severe natural event—**This category includes damage resulting from earthquake, hurricane, tornado, or other severe weather, such as extreme heat, cold, humidity, wind, or drought.
    - **Accidental flood—**Flood causes include pipe leakage from air-conditioning equipment, leakage from a water room on the floor above, fire nozzle being open, accidental triggering of sprinkler systems, broken water main, and open window during rainstorm.
    - **Accidental failure of air conditioning—**Failure, shutdown, or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction, or fail completely.
    - **Electromagnetic radiation—**This can originate from an internal or external device, such as radar, radio antenna, or electricity generating station. This can interfere with proper functioning of equipment or quality of service of wireless transmission and reception.

https://t.me/learningnets

- **Air contaminants—**This is caused by other disasters that produce a secondary problem by polluting the air for a wide geographic area. Natural disasters such as flooding can also result in significant mold or other contamination after the water has receded.

3. Human-caused disasters that hamper business continuity are as follows:
   - Theft of equipment
   - Deliberate fire
   - Deliberate flood
   - Deliberate loss of power supply
   - Deliberate failure of air conditioning
   - Destruction of equipment or media
   - Unauthorized use of equipment
   - Vandalism
4. Four key business components critical to maintaining business continuity are as follows:
   - **Management—**Management continuity is critical to ensure continuity of essential functions. The organization should have a detailed contingency plan indicating a clear line of succession so that designated backup individuals have the authority needed to maintain continuity when key managers are unavailable.
   - **Staff—**All staff should be trained on how to maintain continuity of operations or restore operations in response to an unexpected disruption. In addition, the organization should develop guidelines for vertical and cross training so that staff can take on functions of peers and those above and below them in the reporting hierarchy, as needed.
   - **ICT systems—**Communication systems and technology should be interoperable, robust, and reliable. An organization should identify critical IT systems and have backup and rollover capabilities tested and in place.
   - **Buildings and equipment—**This component includes the buildings where essential functions are performed. Organizations should have separate backup locations available where management and business process functions can continue during disruptions that in some way disable the primary facility. This component also covers essential equipment and utilities.
5. Key steps of business impact analysis are as follows:
   - Inventory key business elements such as business processes, information systems/applications, assets, personnel, and suppliers.
   - Develop intake forms to gather consistent information. Interview key experts throughout the business. Get information from inventories.

https://t.me/learningnets

- Assess and prioritize all business functions and processes, including their interdependencies.
- Identify the potential impact of business disruptions resulting from uncontrolled, nonspecific events on the institution's business functions and processes.
- Identify the legal and regulatory requirements for the institution's business functions and processes. For each business process, determine the maximum tolerable downtime (MTD).
- For each business process, determine a reasonable recovery time objective (RTO) and recovery point objective (RPO). The processes with the shortest MTD or RTO are the most critical business processes. Get agreement from senior management.

6. According to ISO 22301, three key areas to be considered while developing business continuity strategy are as follows:
   - **Protecting prioritized activities—**For activities deemed significant for maintaining continuity, the organization should look at the general strategic question of how each activity is carried out. The goal is to determine a strategy that reduces the risk to the activity.
   - **Stabilizing, continuing, resuming, and recovering prioritized activities and their dependencies and supporting resources—**The next step is to provide more detailed options for managing each prioritized activity during the business continuity process.
   - **Mitigating, responding to, and managing impacts—**In this step, the organization should spell out the strategies that attempt to contain the damage to the organization from disasters.
7. The key objectives of a business continuity awareness program are as follows:
   - Establish objectives of the business continuity management (BCM) awareness and training program.
   - Identify functional awareness and training requirements.
   - Identify appropriate internal and external audiences.
   - Develop awareness and training methodology.
   - Identify, acquire, or develop awareness tools.
   - Identify external awareness opportunities.
   - Oversee the delivery of awareness activities.
   - Establish the foundation for evaluating the effectiveness of the program.
   - Communicate the implications of not conforming to BCM requirements.

https://t.me/learningnets

- Ensure continual improvement of BCM.
- Ensure that personnel are aware of their roles and responsibilities in the BCM program.

8. Business resilience is the ability of an organization to quickly adapt to disruptions while still maintaining continuous business operations and safeguarding people, assets, and overall brand equity. Business resilience has a wider scope than disaster recovery. Business resilience offers post-disaster strategies to avoid costly downtime, to shore up vulnerabilities, and to maintain business operations in the face of additional, unexpected breaches

9. Five sets of organizational continuity controls are as follows:
   - **Business continuity management—**This includes controls that require the organization's business strategies to routinely incorporate business continuity considerations.
   - **Business continuity policy, plans, and procedures—**This requires an organization to have a comprehensive set of documented, current business continuity policies, plans, and procedures that are periodically reviewed and updated.
   - **Test business continuity plan—**This plan incorporates security controls in order to complete a test simulation of the continuity plan to ensure its smooth running if the time comes to implement it.
   - **Sustain business continuity management—**This includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel.
   - **Service providers/third parties business continuity management—**This includes security controls that enforce documented, monitored, and enforced procedures for protecting the organization's information when working with external organizations.

10. Some improvement exercises for participants, as mentioned in an ideal BCP, are as follows:
    - **Seminar exercise (or plan walkthrough)—**The participants are divided into groups to discuss specific issues.
    - **Tabletop exercise—**Participants are given specific roles to perform, either as individuals or groups.
    - **Simple exercise—**This task is a planned rehearsal of a possible incident designed to evaluate the organization's capability to manage that incident and to provide an opportunity to improve the organization's future responses and enhance the competence of those involved.
    - **Drill—**A drill consists of a set of coordinated, supervised activities usually employed to exercise a single specific operation, procedure, or function in a single agency.
    - **Simulation—**This is a type of exercise in which a group of players, usually representing a control center or management team, react to a simulated incident notionally happening elsewhere.

https://t.me/learningnets

- **Live play—**This is an exercise that enables an organization to safely practice the expected response to a real incident.

11. Good business continuity metrics have the following characteristics:
    - Help senior managers (and/or their target audience) quickly see the performance of the response and recovery solutions based on risk to the organization's products and services
    - Convey information that is important to senior managers
    - Focus on performance rather than exclusively on activities
    - Help senior managers identify problem areas to focus attention and remediation efforts
12. In response to a disruptive event, the business continuity process proceeds in three overlapping phases:
    1. **Emergency response—**This phase is focused on arresting or stabilizing an event.
    2. **Crisis management—**This phase is focused on safeguarding the organization.
    3. **Business recovery/restoration—**This phase is focused on fast restoration and recovery of critical business processes.

Chapter 18

1. A security audit is an independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. The key objective of a security audit is to assess the security of the system's physical configuration and environment, software, information handling processes, and user practices.

   A security audit trail is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a security-relevant transaction from inception to final results. Its key objective is to provide a historical record of progression based on a sequence of events to provide proof of compliance and operational integrity.

2. Key elements of the X.816 model for security audit's relationship with security alarms are as follows:
    - **Event discriminator—**This logic embedded into the software of the system monitors system activity and detects security-related events that it has been configured to detect.
    - **Audit recorder—**For each detected event, the event discriminator transmits the information to an audit recorder. The model depicts this transmission as being in the form of a message. The audit could also be done by recording the event in a shared memory area.

https://t.me/learningnets

- **Alarm processor—**Some of the events detected by the event discriminator are defined to be alarm events. For such events, an alarm is issued to an alarm processor. The alarm processor takes some action based on the alarm events and this action is an auditable event that is recorded in the audit recorder.
- **Security audit trail—**The audit recorder creates a formatted record of each event and stores it in the security audit trail.

3. Some of the auditable items suggested in the X.816 model of security audits and alarms are as follows:
   - Security-related events related to a specific connection, such as connection request/confirmation.
   - Security-related events related to the use of security services, such as security service requests.
   - Security-related events related to management, such as management operations/notifications.
   - Events such as access denials, authentication, and attribute changes.
   - Individual security services such as authentication results, access control results, non-repudiation, and integrity responses.
4. There are four types of audit trails:
   - **System-level audit trail—**This type of audit trail is generally used to monitor and optimize system performance but can serve a security audit function as well. The system enforces certain aspects of security policy, such as access to the system itself. A system-level audit trail should capture data such as login attempts, both successful and unsuccessful, devices used, and operating system functions performed.
   - **Application-level audit trail—**Application-level audit trails may be used to detect security violations in an application or to detect flaws in the application's interaction with the system. For critical applications or those that deal with sensitive data, an application-level audit trail can provide the desired level of detail to assess security threats and impacts.
   - **User-level audit trail—**A user-level audit trail traces the activity of individual users over time. It can be used to hold a user accountable for his or her actions. Such audit trails are also useful as input to an analysis program that attempts to define normal versus anomalous behavior.
   - **Physical access audit trail—**This type of audit trail can be generated by equipment that controls physical access and is then transmitted to a central host for subsequent storage and analysis. Examples include card-key systems and alarm systems.

https://t.me/learningnets

5. An external security audit is an independent audit of the security aspects of an organization that is carried out by an external party such as an outsider auditor. Its key objectives are as follows:
   - Assess the process of the internal audit.
   - Determine the commonality and frequency of recurrence of various types of security violations.
   - Identify the common causes.
   - Provide advisory and training inputs to tackle the neglect of procedures.
   - Review and update the policy.
6. The SGP defines the security performance function as follows:
   - **Security monitoring and reporting—**This consists of monitoring security performance regularly and reporting to specific audiences, such as executive management.
   - **Information risk reporting—**This consists of producing reports related to information risk and presenting reporting to executive management on a regular basis.
   - **Information security compliance monitoring—**This consists of information security controls derived from regulatory and legal drivers and contracts used to monitor security compliance.
7. NIST IR 7564 defines the following three broad uses of security metrics:
   - **Strategic support—**Assessments of security properties can be used to aid in different kinds of decision making, such as program planning, resource allocation, and product and service selection.
   - **Quality assurance—**Security metrics can be used during the software development life cycle to eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying likely vulnerabilities, and tracking and analyzing security flaws that are eventually discovered.
   - **Tactical oversight—**Monitoring and reporting of the security status or posture of an IT system can be carried out to determine compliance with security requirements (for example, policies, procedures, regulations), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement.
8. The three key processes for the COBIT 5 Monitor, Evaluate, and Assess domain are as follows:
   - **Performance and conformance—**Collect, validate, and evaluate business, IT, and process goals and metrics. Monitor to ensure that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.

https://t.me/learningnets

- **System of internal control—**Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize, and maintain standards for internal control assessment and assurance activities.
- **Compliance with external requirements—**Evaluate whether IT processes and IT-supported business processes are compliant with laws, regulations, and contractual requirements. Obtain assurance that the requirements were identified and complied with and integrate IT compliance with overall enterprise compliance.

9. COBIT 5 defines the following steps for the performance and conformance process:

    1. **Establish a monitoring approach—**Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope, and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.
    2. **Set performance and conformance targets—**Work with stakeholders to define, periodically review, update, and approve performance and conformance targets within the performance measurement system.
    3. **Collect and process performance and conformance data—**Collect and process timely and accurate data aligned with enterprise approaches.
    4. **Analyze and report performance—**Periodically review and report performance against targets, using a method that provides a succinct all-around view of IT performance and fits within the enterprise monitoring system.
    5. **Ensure the implementation of corrective actions—**Assist stakeholders in identifying, initiating, and tracking corrective actions to address anomalies.

10. SP 800-55 provides the following view of implementing the monitoring and reporting function based on the security performance metrics:

    1. **Prepare for data collection—**This step involves the metrics development process.
    2. **Collect data and analyze results—**The analysis should identify gaps between actual and desired performance, identify reasons for undesired results, and identify areas that require improvement.
    3. **Identify corrective actions—**Based on step 2, determine appropriate corrective actions and prioritize them based on risk mitigation goals.
    4. **Develop business case—**This involves developing a cost model for each corrective action and making a business case for taking that action.
    5. **Obtain resources—**Obtain the needed budget and resource allocation.
    6. **Apply corrective actions—**These actions may include adjustments in management, technical, and operational areas.

https://t.me/learningnets

11. ISACA's guidance on information risk reporting is based on the following two concepts of COBIT 5:

    - **Process—**This is defined as a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs, and produces outputs (for example, products, services). Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.
    - **Activity—**This is the main action taken to operate the process. It provides guidance to achieving management practices for successful governance and management of enterprise IT. It involves describing a set of necessary and sufficient action-oriented implementation steps to achieve a governance practice or management practice.

12. The generic steps for security compliance monitoring are as follows:

    1. Identify key stakeholders and/or partners across the organization who regularly deal with institutional compliance issues (for example, legal, risk management, privacy, audit).
    2. Identify key standards, regulations, contractual commitments, and other areas that address specific requirements for security and privacy.
    3. Perform a high-level gap analysis of each compliance requirement that is applicable to determine where progress needs to be made.
    4. Develop a prioritized action plan to help organize remedial efforts.
    5. Develop a compliance policy, standard, roles and responsibilities, and/or procedures in collaboration with other key stakeholders.

https://t.me/learningnets