EC-Council

C|CISO

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

VERSION 3

Join the New Generation of Information Security Leaders

Certified Chief Information Security Officer

hide01.ir

ALL RIGHTS RESERVED.

No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

The C|CISO logo is protected by the United State Patent and Trademark Office under registration number 4,175,755.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein or perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use or reliance of this material.

hide01.ir

C|CISO BODY OF KNOWLEDGE

EC-Council Executive Management:

Sanjay Bavisi, President

Steven Graham, Sr. Vice President

Sean Lim, Sr. Vice President

Eric Lopez, Vice President

EC-Council C|CISO Body of Knowledge Editing and Management:

Keith Rayle, Senior Director of C|CISO

Authored By:

Keith Rayle, Senior Director of C|CISO

Chris Campbell, Sr. Director of Information Security public company, Committee Chair EC-Council BOK Committee

Vincent Lewis, Cloud Security Engineer Information System Security Manager, Dept. of the U.S. Air Force, Committee Vice-Chair EC-Council BOK Committee

Ayodeji Akinola, Senior Security Consultant for Mariner Partners Inc.

Jeffrey Aschenbach, Chief Information Security and Privacy Officer, Cooler Screens Inc.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Dr. Jerry Craig, Chief Information Security Officer, Ntiva, Inc

Dr. Thomas "Tom" Duffey, ITEGRITI Director Cybersecurity and Compliance

Justen Dyche, Head of Information Security Delivery, BBC

Brandon Gettert, Founder and CEO of Curated Cyber

Jorge L Gomez, Cloud Security Architect/Engineer, Twilio

Corlette Grobler, Chief Information Security Officer, HAYVN

Karin Höne, Group Chief Information Security and Risk Officer at a South African multinational

Federico Iaschi, Head of Cyber Security Resilience & Observability, Virgin Media 02

Jari Kiero, Senior Resilience Officer, Allianz Technology SE

Paul Lynch, Senior Director of Information Security and Infrastructure, CubeSmart Self Storage

Peter Pandula, Senior Advisor, BMO Financial Group

Daniel Pinsky, CSO & Head of Security Governance and Compliance, CDW Canada

Keyaan Williams, Managing Director, CLASS-LLC

Bjoern Voitel, Owner and CEO of three information security companies

hide01.ir

Edited By:

Keith Rayle, Senior Director of C|CISO

Vincent Lewis, Cloud Security Engineer Information System Security Manager, Dept. of the U.S. Air Force, Committee Vice-Chair EC-Council BOK Committee

Chris Campbell, Sr. Director of Information Security public company, Committee Chair EC-Council BOK Committee

Ayodeji Akinola, Senior Security Consultant for Mariner Partners Inc.

Jorge L Gomez, Cloud Security Architect/Engineer, Twilio

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Preface

The advancement of the security executive role in corporate governance has followed proportionately with the increase in criminal activities focused on critical data and systems supporting public and private organizations. The velocity, creativity, and focus of cyberattacks continues to escalate, resulting in the need for clear executive leadership that delivers the ability to enable resilient business outcomes. Within two decades, the role of the Chief Information Security Officer has grown from being rarely seen beyond financial or government institutions to the current state in which many globally recognized regulatory agencies specify the presence of strategic security leadership to satisfy compliance requirements. A properly functioning security capability has become critical for the successful transaction of all forms of business. Security executives are now required to apply clearly defined, organizationally aligned portfolios that deliver focused capabilities to identify, communicate, and manage cyber risk according to the needs of the organization. Fulfilling the role of a leader within the security industry requires the ability to orchestrate people, technologies, and processes into a highly functioning, highly efficient portfolio of services and capabilities purposefully implemented to protect critical assets.

Today's Chief Information Security Officer must rely on a wide range of tools to be successful. True security leadership requires deep dedication to the security industry, years of technical and non-technical security program experience, visibility into the constantly changing threat landscape, and the ability to create strategies and implement them according to a carefully planned schedule. Successful security executives also need deep knowledge of business operations, a wide perspective of industry trends, strong leadership capabilities, and communications skills that are effective throughout all organizational levels and up to the Board of Directors.

EC Council's C|CISO Program is defined, designed, and delivered by seasoned security executives. The dozens of individuals that contribute their time and knowledge for this program have led security teams, created strategies, regularly briefed at the Board level, and delivered complex capabilities orchestrated to protect critical assets and infrastructure. Their dedication to the security profession is evident within the materials of the C|CISO Program. EC Council's dynamic knowledge model and delivery methodology not only provides you with the necessary tools to realize your career goals, but also provides assurance of the value of this certification through the hundreds of years of deep security leadership experience behind this program.

Welcome to your future as a security industry leader.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Foreword

A 2023 Perspective

Hello to my fellow global C|CISOs!

2023 was an interesting year full of challenges for security executives for a variety of different reasons. The most interesting shift (in my opinion) from our perspective was not necessarily encapsulated within the topics of technology, cyberattacks, or changes in the demand for security expertise. Don't get me wrong – they were all important factors within the security landscape of 2023.

Technology certainly advanced, providing a wide range of new ideas that, over time, will resolve into stand-alone mainstream solutions or become integrated into similar verticals of products. However, I think the velocity of those types of changes has been somewhat predictable and certainly provide security professionals with the usual choices…adopt early, delay until a certain degree of maturity exists, or 'wait-and-see' to determine if the technology matures into steady mainstream usage. It seems that technology was relatively consistent with what one would expect to see from an innovation perspective. One example is cloud technologies. Cloud security capabilities, such as security management platforms, instance baseline templates, and access brokering have become mainstream and are often 'baked in' to the foundational cloud vendor offering. Another technology, Artificial Intelligence (AI), has been integrated into a wide range of products (or, in some cases, only the marketing materials). Quantum computing is mostly relegated to research while stability issues are resolved, hindering availability of commercially viable platforms. Overall, I do not see a technology that has radically redefined our approach to security in this past year.

Criminal activities have remained relatively consistent with expectations, and ransomware leads the list of cyber concerns from the business perspective (much as it has for the past few years). There are some advances, but nothing apart from what one would expect. More successful attacks are being experienced (and particularly at the lower end of the business-size scale), payouts are larger, the attacks are more violent and vicious in nature, and cybercriminal organizations seem more…organized. But the primary methodology of a successful ransomware attack remains relatively consistent: successful phishing or other unauthorized access attack allows vulnerable technology implementations to be leveraged for broader manipulation of critical systems and information. Digital currencies still enable transactional ransom resolution. Meantime, nation/state actors continue to increase their negative global impact as they continue stealing national secrets, intellectual property, and personal information. Some are certainly better at it than others, but activity continues along a somewhat expected trend line of proliferation and capability.

Security expertise shortages continued throughout 2023, with most open labor requisition estimates following trends as we have seen for the past 10 years. Clusters of technologies, such as cloud, continue to morph and evolve, but demand for security professionals within the tech towers seems to have remained relatively constant. Worth noting is an estimated 333K technology workers were laid off over the 22-month period of January 2022 through October of 2023. My suspicion for cause is the mainstream and rapid transition to cloud as a primary factor. This shift appears to have created pockets of competition for open security roles that can make the shortage appear somewhat antithetical. Artificial Intelligence (AI) is hitting stride, but security skills specifically focused on it do not represent

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

a major shift in the percentages of high-demand security skills within this industry. Core capabilities and resources, such as security analysts, risk program resources, forensics experts, and others, fall into similar demand as we have seen in the recent past.

Security management has not radically changed. Organizations still need executives that can create and integrate strategies that align closely to the business goals while meeting the needs of the workforce, senior leadership, and the Board of Directors. Chief Information Security Officers communicate in terms of risk to the business and advise accordingly. Regulatory measures regarding security and privacy increase at an expected rate. Security executives build programs based on relatively static frameworks and standards. Security executives still manage their security program regardless of resource challenges. The trend towards DevOps and DevSecOps continues, underscoring the importance of security leadership working collaboratively with their software development and engineering counterparts to enable cyber risk controls within applications and cloud-centric environments. There is one thing that has changed in the past couple of years from a leadership perspective – the need to effectively deliver the portfolio of security services using, for the most part, a distributed workforce.

I think the most significant recent change impacting the security landscape was the safe enablement of the decentralized workforce. The 2020 pandemic has, for all practical purposes, changed the business operational model significantly (and, it appears, permanently). As a rule (with exceptions, of course), employees no longer spend the hour or so to get ready for the day and commute to a mandatory place of work, then leave the workplace for the day. Now they log in remotely from the house, apartment, or some other convenient location. They communicate via email and instant chat, collectively gather as groups using online meetings, and use collaboration tools to rapidly accept and complete assignments individually or within groups. And they can do this from anywhere.

We have had Work-From-Home (WFH) capabilities for years, but they have now become centrally critical to conducting business and retaining skilled resources. We have settled into the new norm.

2023 brought about the implementation and overall user community acceptance of integrated security controls supporting the WFH model. Security solutions focused on remote endpoints have deployed at an accelerated and expanded pace, being pushed downward into smaller sized organizations and throughout all levels of business sizes. Safe remote connection was enabled through the implementation of security guardrails within externally facing services such as VPN, web services, and remote desktop protocols. We leveraged virtualized environments on a much broader scale. Multi-Factor Authentication (MFA) is nothing new but is foundational for securing the WFH model. We are seeing a shift to password-less authentication models to further ease password fatigue among remote workers - while retaining MFA levels of protection.

Endpoint Detection and Response, coupled with managed services (EDR/MDR), has become mainstream. An interesting shift in thinking has occurred due to expanded MDR adoption. We have come to terms with integrating external entities into another facet of operational security models. Security professionals and the broader business have more readily embraced 3rd party monitoring, management, and issue containment at the mobile endpoint (to include BYOD).

Mobile device management is used not only to protect sensitive corporate data, but it is also being leveraged to push other controls such as removing local administrative rights, pushing rapid patches and updates across OS and applications, and forcing regular reboots and sign-ins. Through endpoint management systems we have deeper visibility into the security status of our user base and faster access to logs for analysis of potential issues.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

I think 2023 was the year of maturing and integrating foundational endpoint security in support of the WFH model. Let's see what 2024 brings.

Keith Rayle

Senior Director, C|CISO Program

November 2023

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The EC-Council Certified CISO Program

EC-Council developed the Certified Chief Information Security Officer (C|CISO) Program to fill a gap within the information security industry. At that time, security certifications focused on technical skills, historic security perspectives, specific tools, or narrow practitioner responsibilities such as risk or compliance program support. There needed to be a clear path from security practitioner to the executive leadership role. No certifications recognized the knowledge, skills, and capabilities required of the security executive role. More shared knowledge was needed to direct experienced information security professionals to the level of performing the duties of an effective, competent security industry leader. At that time, there were more questions than answers about what being a CISO meant. It wasn't easy to communicate the real value of the security executive's contribution to an organization's success.

EC-Council created the C|CISO Program to bridge the gap within the security profession and enable a clear path to the role of an executive-level security professional. This certification is aligned closely with the overall leadership trend of the security industry. Today, the CISO is a global business enabler, creating information risk management capabilities that help define organizational strategies and success factors. International laws, regulations, and standards often mandate the security leadership role. EC-Council's C|CISO Program meets the needs of the security leadership profession by providing the tools, knowledge, and capabilities to protect against today's cyber threats.

The C|CISO Program uses four core pillars of knowledge transference to enable qualified individuals wishing to attain this certification. They include classroom instruction, a blueprint for defining an organized hierarchy of C|CISO capabilities, the certification examination, and this Body of Knowledge.

hide01.ir

The Body of Knowledge represents the foundational skills and knowledge required to be a successful security executive. It also represents decades of direct security leadership experience provided by the C|CISO Body of Knowledge Committee, which consists of current C|CISOs and seasoned security executives from multiple industries and regions worldwide. With their input to this Body of Knowledge, these experts provide a clear view into the C|CISO role and security program capabilities this person needs to deliver within an organization.

The C|CISO Program consists of five domains that provide deeper insight into the foundational capabilities of a successful security executive:

- Domain 1 – Governance & Risk Management (Policy, Legal & Compliance)
- Domain 2 – Information Security Controls, Compliance, and Audit Management
- Domain 3 – Security Program Management and Operations
- Domain 4 – Information Security Core Competencies
- Domain 5 – Strategic Planning, Finance, Procurement and Vendor Management

The details within these five domains of the C|CISO Program provide the basis for being an effective information security program leader.

EC-Council enhances this program by offering additional professional insight from certified instructors via in-classroom, remote attendance, or self-study (video) training. Materials used for instruction, like this Body of Knowledge, are maintained by a committee of deeply experienced security executives with the C|CISO title. A global community of professional instructors actively

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

teaches the C|CISO course, imparting knowledge based on years of experience within the security leadership profession.

EC-Council then evaluates the knowledge of C|CISO candidates with a rigorous exam that evaluates competence across the five domains representing a seasoned security leader's knowledge base. The C|CISO Examination Committee, also consisting of deeply experienced C|CISOs, creates questions for use within the tests. These questions are based on their knowledge of all C|CISO Program materials and years of executive leadership experience in security.

The C|CISO Scheme Committee provides two primary functions. The C|CISOs within it maintain the C|CISO Blueprint and Job Task Analysis catalogs of the knowledge required by security executives. This committee, consisting of C|CISOs with deep leadership experience, reviews and approves questions for inclusion in the C|CISO certification examination.

The C|CISO Program was the first to offer a security industry certification recognizing an individual's accumulated skills for developing, executing, and leading an information security management strategy. The C|CISO certification demonstrates an information security leader's commitment to the profession. It provides assurance they have the foundational knowledge and skills to help protect the organization against the ever-growing attacks against critical infrastructure and data. C|CISOs know how to identify and communicate risk, implement security strategies, adapt to threats, and align security programs to broader strategic goals. EC-Council C|CISOs are the critical leadership component for protecting globally connected organizations and businesses.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Acknowledgments

While many people contributed to this Body of Knowledge, the EC-Council would like to thank the principal authors of the work.

Keith Rayle

Keith has functioned as CISO in large multinational corporations, designed and implemented security governance programs, and created risk management approaches for organization operations and specific programs such as large mergers and acquisitions.

Keith advises multibillion-dollar private equity firms and has delivered multimillion-dollar security engagements comprised of multiple discreet technical and non-technical projects. He has provided executive security consulting in every industry on a global basis. Keith has a Bachelor of Science degree in Computer Science and a Master of Science degree in Information Systems.

Chris Campbell

As chairperson for the EC-Council Body of Knowledge Committee, Chris brings seasoned information security leadership with over 23 years of experience in technology and cybersecurity across the energy, financial, and real estate sectors. He is currently the Senior Director and Head of Information Security and Compliance for a publicly traded financial technology company.

He was previously a cybersecurity leader for a Fortune 150 energy company within the U.S. critical infrastructure. He has an M.S. in Management Information Systems and a B.A. in Finance and Marketing from Florida International University. He holds the C|CISO, CISM, CRISC, CDPSE, CISA, CISSP, CHFI, and GCIH industry certifications.

Vincent Lewis

Committee Vice-Chair for the EC-Council Body of Knowledge Committee, Vincent is a United States Air Force retired IRAQI war veteran with over 23 years of cyber security experience. He currently performs the role of Cloud Security Engineer and Information System Security Manager for the Department of the Air Force, protecting government information traversing commercial cloud providers. He also performed the NIST Risk Management Framework, governance, compliance, and regulation work for the Department of the Air Force global cloud instances.

He has a Master of Arts degree in Management and Leadership with an emphasis in Cybersecurity, a Master of Science degree in Cybersecurity, a Graduate level certificate in cyber threat detection, and a bachelor's degree in information technology. He holds the C|CISO, CISSP, Security+, and Microsoft Certified Professional industry certifications.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Ayodeji Akinola

Ayodeji is an Information Technology enthusiast with a bias for security and over 20 years of experience working across various verticals, including telecommunications, insurance, and finance. He currently works as a senior security consultant for Mariner Partners Inc. Earlier in his career, he worked for IBM and Wipro Limited in various roles.

He graduated from Obafemi Awolowo University, Nigeria, with a bachelor's degree in civil engineering. He has since pivoted fully into Information Technology and Security. He holds industry certifications such as the C|CISO, C|EH, CISSP, Microsoft Certified: Azure Solutions Architect Expert, and AWS Certified Solutions Architect – Associate, amongst others. He is also PMP certified.

Jeffrey Aschenbach

Jeffrey is an accomplished Information Security, Compliance, and Data Privacy leader with over 20 years of experience in the financial service, healthcare, manufacturing, and, most recently, advertising industries. He currently sits as the Chief Information Security and Privacy Officer for Cooler Screens Inc.

Before joining Cooler Screens, he was an influential Vice President of Global IT Security for Mediaocean, a Vista Equity Partners Company. He has a B.S. in Organizational Leadership and Supervision with an emphasis on Computer Information Systems Technology from Purdue University. He holds the C|CISO, CISSP, and CISA industry certifications.

hide01.ir

Dr. Jerry Craig

A 20+ year IT management and security career recognized for innovation and strategic direction. Dr. Craig is the Chief Information Security Officer (CISO) at Ntiva, Inc., a large Managed Service Provider (MSP) based out of the Northern Virginia area, where he serves as the corporate CISO, as well as a virtual CISO to his clients. He was formerly the Vice President of Security Systems for a $1B+ intellectual property-led healthcare solutions provider. Dr. Craig has led a distinguished career driving concurrent programs and projects and building and leading teams of security professionals. He is recognized for developing and implementing strategies for growth while reducing organizational risk and expenditures.

Dr. Craig is a trusted advisor to CEOs, Boards of Directors, and C-Suite executives. In addition to his IT career, Dr. Craig has a 14+ year career in higher education, supporting multiple universities with student recruitment and teaching and providing positive mentorship outreach to ensure student success and inspire the next generation of leaders. Dr. Craig informally serves as a Chief Data Officer (CDO) and Chief Privacy Officer (CPO) for numerous clients and extensively participates on the Business Development Team supporting proposal efforts.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Dr. Thomas "Tom" Duffey

ITEGRITI Director of Cybersecurity and Compliance. Dr. Tom specializes in critical infrastructure cybersecurity and regulatory compliance for the energy (utilities and oil & gas), defense, and healthcare sectors. He has over 30 years of experience in different roles and is passionate about protecting operational technology (OT) and the Internet of Things (IoT) for various industries. Dr. Tom's diverse consulting, training, and project management experience also includes supporting multiple military branches at numerous CONUS and OCONUS facilities across the globe. Dr. Tom currently resides in Houston, where he leads OT/IT/IoT critical infrastructure protection delivery efforts for multiple ITEGRITI clients, assisting them with their cybersecurity and compliance needs, including NERC CIP and TSA SD02 regulatory criteria.

Teaching and learning are two of Dr. Tom's biggest passions. He contributed to numerous security thought leadership efforts, including co-authoring a World Economic Forum whitepaper and co-leading domain rewrites for the EC-Council C|CISO Body of Knowledge. Dr. Tom earned his Doctoral degree in Computer and Information Security, authoring a dissertation exploring the impact of NERC CIP regulatory compliance on security and risk. Dr. Tom currently also participates in various NERC/TSA-related efforts and supporting roles, including Education Director for ISSA South Texas, Meeting Logistics Director for the Houston InfraGard Energy Cross-Sector Council, NERC Supply Chain Working Group Vice Chair, Co-Education Lead for Houston ISACA, and Houston ISA Assistant Education Director. Recently, he presented on NERC/TSA compliance at the 2023 Houston API cybersecurity conference.

hide01.ir

Justen Dyche

Justen has been a media professional for over 30 years. He has been responsible for delivering Information Security to the BBC for the past eight years. Currently Head of Strategy, he is responsible for creating and maintaining the information security strategy, ensuring alignment with a continually evolving BBC operating model that reflects the corporation's leading role in the modern digital-first media sector.

Justen recently led an ambitious transformation program that fundamentally re-engineered the BBC's InfoSec provision: designing and delivering a clear and comprehensive strategic framework underpinned by tailored tools and processes that capture and exploit a rich data set. The program drove culture change across the department, gaining recognition in the SC Awards 2022. Justen was honored in the C|CISO Hall of Fame in 2023 and holds C|CISO, C|EH, CISSP, CCSP, CGRC, CISM, CRISC, CISA, and ISO27001 Lead Auditor industry certifications.

Brandon Gettert

Brandon is a seasoned cybersecurity expert with 24 years of experience spanning compliance, governance, networking, IT infrastructure, and management. Renowned for his ability to identify and mitigate risks, he specializes in ethical hacking, vendor management, and information security program development. As a gifted communicator and educator, Brandon is a sought-after speaker on cybersecurity topics nationwide.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

He is the founder and CEO of Curated Cyber, managing a team of vCISOs, and the founder and President at Lithium Advisors, a cybersecurity board advisory service. Additionally, he teaches at Elite CEU, leveraging his broad experience in financial services, education, the public sector, and software development to offer real-world insights. Brandon is an industry leader, innovator, and educator dedicated to advancing the cybersecurity field.

Jorge L Gomez

Jorge is a cybersecurity professional with over 15 years of practical experience in the energy, financial, cloud infrastructure, and technology industries. He has led and matured numerous cybersecurity programs, including identity & access management, incident response, threat intelligence, security architecture & engineering, application/product security, and cloud security.

More recently, he has become a specialist in the cloud and product security domains by applying a pragmatic approach and focusing on developer-first security practices. He studied at the University of Miami and holds Electrical and Computer Engineering degrees.

Corlette Grobler

Over two decades of IT experience, including experience in executive and management positions in multinational corporations across various industries, including Banking, Financial Services, Retail, Logistics, and Telecommunications. For the past five years, she has been focused intently on Information Security.

She is pursuing a Master of Science degree in Cybersecurity through the University of Liverpool's correspondence program, intending to acquire advanced specialist skills and knowledge to better mitigate the increasing threat of cyberattacks.

Over the past three years, she successfully designed a comprehensive Cybersecurity Awareness Programme (Bank) to increase cybersecurity awareness among end users through various channels such as email, intranet, posters, and mandatory training courses. The program included social engineering simulations, such as phishing, SMS, and whaling attacks, to boost users' awareness. In addition, she has made significant contributions to the design and development of a DevSecOps maturity analysis tool for a major South African Bank. She has also played a key role in crafting the business and technology architecture for a multinational insurance organization with a strong focus on security. She is currently assisting a major bank with its cloud adoption journey, with a specific emphasis on FinOps and cybersecurity.

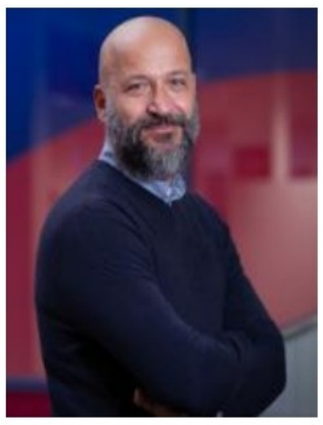
Karin Höne

Karin is an enthusiastic IT Security and Risk professional with more than 20 years of experience in the industry in various roles. She currently holds the position of Group Chief Information Security and Risk Officer at a South African multinational. In her role, she challenges herself to craft easy-to-understand IT security and risk strategies linked to the business challenges and objectives of the

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

day. These strategies support executive and board reporting that makes the IT Security and Risk topic accessible and demonstrates the value of the discipline.

Her other area of focus is demystifying IT risk and ensuring risk ownership is understood and placed where it belongs. Karin holds a master's degree in informatics (cum laude) specializing in information security from the Rand Afrikaans University. She holds the certifications of C|CISO, CISSP, and AMBCI. She has received numerous global accolades, such as being inducted into the 2022 – 2023 Certified CISO Hall of Fame and included in various global Top 100 CISO lists in 2022 and 2023.



Federico Iaschi

A seasoned leader in information security and risk management, with a combination of leadership, technical, and managerial experience developed over 20 years within private and public sector enterprises with global and local companies.

He combines multifaceted business insight with excellent interpersonal and leadership skills to build trusting relationships and deliver strong personal and team results. During his career, Federico has achieved extensive professional certifications such as C|CISO, CISSP, CISM, CGEIT, CRISC, CDPSE, ISO27001 LA, and more. He regularly presents at conferences and industry events and assists in writing industry certification material.

Jari Kiero

Jari has worked in information technology for over 25 years, guiding organizations in protecting their most important assets against various threats. He has served in various management positions at well-known IT services, telecommunications, manufacturing, and insurance companies. Currently, he is working on digital operational resilience topics, anticipating and formulating scenarios from risk management and cyber resilience perspectives.

hide01.ir

Jari holds a master's degree in industrial engineering and management from the Lappeenranta University of Technology and a second master's in human factors in manufacturing systems from the University of Nottingham. Additionally, he has obtained 15 industry certifications, including C|CISO, CISM, C|EH, CISSP, CCSP, CISA, and ITIL 4 Managing Professional.

Paul Lynch

Paul is currently the Senior Director of Information Security and Infrastructure for CubeSmart Self Storage. He has more than 20 years of experience in information technology. He has established security governance programs and best practices for government, non-profit, private, and publicly traded organizations ranging from technology startups to city governments.

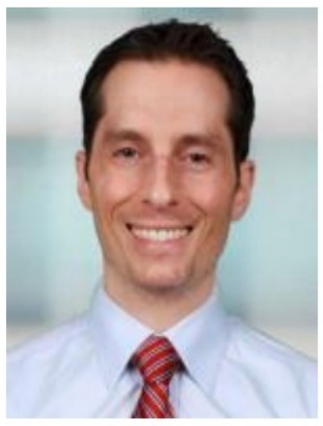
He holds several information security certifications, including C|CISO, CISSP, ISSMP, and CCSP. He has served as an exam content subject matter expert for EC-Council and (ISC)2, specializing in security governance and cloud security. He serves on the Customer Advisory Board for both eSentire and Lacework.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Peter Pandula

Peter has over 25 years of industry experience and works at BMO Financial Group. He earned his master's degrees in psychology, Physics, Computer Science, and Business Administration.

He holds industry certifications and credentials in project management, investment management, marketing, risk management, artificial intelligence, information technology (IT) governance, emergency management leadership, payment card cybersecurity, and information security.

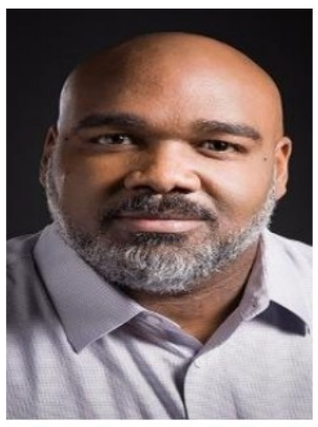


Daniel Pinsky

Daniel is a seasoned cybersecurity leader with over 23 years of experience. He has worked across various industries and sectors in North America and Europe, showcasing his expertise in governance, program development, and implementing and certifying different control frameworks.

Currently, Daniel leads the national cybersecurity program and serves as the CSO for a Fortune 200 company. He earned his degree from McGill University, where he studied business and technology. He has multiple certifications, including C|CISO, CISM, CISA, and CISSP.

Daniel's enthusiasm extends to leadership, effective communication, and personal development. He generously shares his insights and wisdom through various mediums, including writing, public speaking, and mentoring.



Keyaan Williams

Keyaan J Williams has been building and managing cybersecurity and privacy programs to support enterprise risk management for more than two decades. After many years in various departments of the Centers for Disease Control and Prevention (CDC), he started a global consulting firm that supports government, critical infrastructure, and commercial customers. Keyaan actively serves as a board member for commercial and non-profit companies. He also serves as a mentor and advisor for corporate directors and early-stage entrepreneurs.

He regularly shares interesting insights on LinkedIn based on ideas he has published in books and professional journals.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bjoern Voitel

Bjoern is a privacy and information security professional with over 20 years of experience in several fields, including the financial and critical infrastructure sectors and public and governmental agencies. He is the owner and CEO of three information security companies. He is also a penetration tester and seasoned instructor for EC-Council, ISC², ISACA, Offensive Security, and CompTIA.

He has a diploma in business administration (with a focus on information systems) from the University of Osnabrueck. He holds the C|CISO, CPENT, C|EH Master, CND, CSA, CISM, CRISC, CDPSE, CISA, CGEIT, CISSP-ISSAP, CCSP, CCSLP, SSCP, OSCP and ISO 27001 Lead Auditor industry certifications.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Copyright 2

Preface 4

Foreword 5

The EC-Council Certified CISO Program 8

Acknowledgments 10

Table of Contents 17

List of Figures 23

List of Tables 25

Domain 1: Governance & Risk Management (Policy, Legal & Compliance) 1

Governance 2

Knowledge Assumptions 2

1. DEFINE, IMPLEMENT, MANAGE, AND MAINTAIN AN INFORMATION SECURITY GOVERNANCE PROGRAM 3

1.1. Form of Business Organization 3
1.2. Industry 4
1.3. Organizational Maturity 4

2. INFORMATION SECURITY DRIVERS 5

3. ESTABLISHING AN INFORMATION SECURITY MANAGEMENT STRUCTURE 6

3.1. Organizational Structure 6
3.2. Where does the CISO fit within the organizational structure? 6
3.3. The Executive CISO 7
3.4. C-Level Attitudes toward the CISO 7
3.5. Nonexecutive CISO 7

4. LAWS/REGULATIONS/STANDARDS AS DRIVERS OF ORGANIZATIONAL 8

4.1. POLICY/STANDARDS/PROCEDURES 8

5. MANAGING AN ENTERPRISE INFORMATION SECURITY COMPLIANCE PROGRAM 9

5.1. Security Policy 9
5.2. Policy Content 11
5.3. Reporting Structure 16
5.4. Standards and Best Practices 16
5.5. Leadership and Ethics 17
5.6. EC-Council Code of Ethics 18

6. INTRODUCTION TO RISK MANAGEMENT 19

6.1. Risk Management Standards 20

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.2. The Essentials of a Risk Management Program 21
6.3. Where Risk Resides 23
6.4. Risk Ownership 23
6.5. Risk Assessment Types 24
6.6. Risk Assessment Process 24
6.7. Risk Categories 26
6.8. Risk Treatment 27
6.9. Risk Modification 30
6.10. Risk Treatment Options 33
6.11. Applying Compensating Controls to Reduce Risk 36
6.12. Risk Calculation Formula 36
6.13. Risk Management Frameworks 37
6.14. NIST Risk Management Framework (RMF) 45
6.15. NIST Risk Management and Assessment 47
6.16. NIST Risk Management Hierarchy 48
6.17. NIST Risk Assessment Process 48
6.18. Other Frameworks 50
6.19. Risk Management Policies and Procedures 54
6.20. Risk Management Lifecycle 56
6.21. Risk Management Program Implementation Use Case 58
6.22. Risk Management Program Review 63

7. SUMMARY 64

Domain 2: Information Security Controls, Compliance and Audit Management 66

Introduction 67

Knowledge Assumptions 67

1. INFORMATION SECURITY CONTROLS 68
1.1. Identifying the Organization's Information Security Needs 68

2. COMPLIANCE MANAGEMENT 83
2.1. Acts, Laws, and Statutes 84
2.2. Regulations 86
2.3. Standards 87

3. GUIDELINES, GOOD AND BEST PRACTICES 99
3.1. CIS 99
3.2. OWASP 100

4. AUDIT MANAGEMENT 100
4.1. Audit Expectations and Outcomes 101
4.2. IS Audit Practices 101

5. SUMMARY 114

Domain 3: Security Program Management and Operations 115

Introduction 116

Knowledge Assumptions 116

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. PROGRAM MANAGEMENT 117
1.1. Defining a Security Charter, Objectives, Requirements, Stakeholders, and Strategies 117
1.2. Executing an Information Security Program 122
1.3. Defining and Developing, Managing and Monitoring the Information Security Program 122
1.4. Defining and Developing Information Security Program Staffing Requirements 126
1.5. Managing the People of a Security Program 128
1.6. Managing the Architecture and Roadmap of the Security Program 131
1.7. Program Management and Governance 132
1.8. Business Continuity Management (BCM) and Disaster Recovery Planning (DRP) 135
1.9. Data Backup and Recovery 135
1.10. Backup Strategy 136
1.11. ISO BCM Standards 136
1.12. Continuity of Security Operations 141
1.13. BCM Plan Testing 141
1.14. DRP Testing 142
1.15. Contingency Planning, Operations, and Testing Programs to Mitigate Risk and Meet Service Level Agreements (SLAs) 142
1.16. Computer Incident Response (aka Cyber Incident Response) 142
1.17. Digital Forensics 145
2. OPERATIONS MANAGEMENT 148
2.1. Establishing and Operating a Security Operations (SecOps) Capability 148
2.2. Security Monitoring and Security Information and Event Management (SIEM) 149
2.3. Event Management 150
2.4. Incident Response Model 153
2.5. Threat Management 156
2.6. Threat Intelligence 157
2.7. Vulnerability Management 158
2.8. Threat Hunting 163
3. SUMMARY 165

Domain 4: Information Security Core Competencies 166
Introduction 167
Knowledge Assumptions 167
1. ACCESS CONTROL 168
1.1. Authentication, Authorization, and Auditing 168
1.2. Authentication 169
1.3. Authorization 171
1.4. Auditing 172
1.5. User Access Control Restrictions 172
1.6. User Access Behavior Management 173
1.7. Types of Access Control Models 173
1.8. Designing an Access Control Plan 175
1.9. Access Administration 175
2. PHYSICAL SECURITY 177
2.1. Designing, Implementing, and Managing a Physical Security Program 177

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2.2. Physical Location Considerations 177
2.3. Obstacles and Prevention 178
2.4. Secure Facility Design 179
2.5. Preparing for Physical Security Audits 182

3. NETWORK SECURITY 182
3.1. Network Security Assessments and Planning 182
3.2. Network Security Architecture Challenges 183
3.3. Network Security Design 183
3.4. Network Standards, Protocols, and Controls 183
3.5. Wireless (Wi-Fi) Security 192
3.6. Voice over IP Security 193

4. ENDPOINT PROTECTION 193
4.1. Endpoint Threats 194
4.2. Endpoint Vulnerabilities 195
4.3. End User Security Awareness 195
4.4. Endpoint Device Hardening 196
4.5. Endpoint Device Logging 196
4.6. Mobile Device Security 196
4.7. Internet of Things Security (IoT) 198

5. APPLICATION SECURITY 200
5.1. Secure SDLC Model 200
5.2. Separation of Development, Test, and Production Environments 200
5.3. Application Security Testing Approaches 201
5.4. DevSecOps 201
5.5. Waterfall Methodology and Security 203
5.6. Agile Methodology and Security 204
5.7. Other Application Development Approaches 204
5.8. Application Hardening 204
5.9. Application Security Technologies 205
5.10. Version Control and Patch Management 205
5.11. Database Security 206
5.12. Database Hardening 207
5.13. Secure Coding Practices 207

6. ENCRYPTION TECHNOLOGIES 208
6.1. Encryption and Decryption 208
6.2. Cryptosystems 208
6.3. Hashing 210
6.4. Encryption Algorithms 210
6.5. Encryption Strategy Development 211

7. VIRTUALIZATION SECURITY 214
7.1. Virtualization Overview 214
7.2. Virtualization Risks 215
7.3. Virtualization Security Concerns 216
7.4. Virtualization Security Controls 216
7.5. Virtualization Security Reference Model 217

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. CLOUD COMPUTING SECURITY 218
8.1. Overview of Cloud Computing 218
8.2. Security and Resiliency Cloud Services 220
8.3. Cloud Security Concerns 220
8.4. Cloud Security Controls 222
8.5. Cloud Computing Protection Considerations [104] 222
9. TRANSFORMATIVE TECHNOLOGIES 224
9.1. Artificial Intelligence 224
9.2. Augmented Reality 224
9.3. Autonomous SOC 225
9.4. Dynamic Deception 225
9.5. Software-Defined Cybersecurity 226
10. SUMMARY 226

Domain 5: Strategic Planning, Finance, Procurement and Vendor Management 228
Introduction 229
Knowledge Assumptions 229
1. STRATEGIC PLANNING 230
1.1. Understanding the Organization 231
1.2. Creating an Information Security Strategic Plan 235
2. DESIGNING, DEVELOPING, AND MAINTAINING AN ENTERPRISE INFORMATION SECURITY PROGRAM 241
2.1. Ensuring a Sound Program Foundation 242
2.2. Architectural Views 242
2.3. Creating Measurements and Metrics 243
2.4. Balanced Scorecard 244
2.5. Continuous Monitoring and Reporting Outcomes 244
2.6. Continuous Improvement 246
2.7. Information Technology Infrastructure Library (ITIL) Continual Service Improvement (CSI) 246
3. UNDERSTANDING THE ENTERPRISE ARCHITECTURE (EA) 247
3.1. EA Types 248
4. FINANCE 254
4.1. Understanding Security Program Funding 254
4.2. Analyzing, Forecasting, and Developing a Security Budget 254
4.3. Managing the information Security Budget 259
5. PROCUREMENT 262
5.1. Procurement Program Terms and Concepts 262
5.2. Understanding the Organization's Procurement Program 263
5.3. Procurement Risk Management 265
6. VENDOR MANAGEMENT 266
6.1. Understanding the Organization's Acquisition Policies and Procedures 266
6.2. Applying Cost-Benefit Analysis (CBA) During the Procurement Process 268
6.3. Vendor Management Policies 269
6.4. Contract Administration Policies 269

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.5. Delivery Assurance _____ 271

7. SUMMARY _____ 272

References _____ 273

INDEX _____ 283

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

List of Figures

FIGURE 1: CMMI MODEL OUTLINE 4
FIGURE 2: ORGANIZATIONAL STRUCTURE 7
FIGURE 3: INFORMATION SECURITY MANAGEMENT SYSTEM/FRAMEWORK 9
FIGURE 4: RISK MANAGEMENT STANDARDS 20
FIGURE 5: RISK MANAGEMENT. SOURCE: "THE ESSENTIALS OF RISK MANAGEMENT" 22
FIGURE 6: RISK CONFLUENCE DIAGRAM 23
FIGURE 7: RESIDUAL RISK FORMULA 27
FIGURE 8: ISO 27005 RISK TREATMENT ACTIVITY 29
FIGURE 9: RISK TREATMENT OPTIONS 33
FIGURE 10: ISO 27005 RISK MANAGEMENT PROCESS 39
FIGURE 11: ISO 27005 PROCESS WORKFLOW 41
FIGURE 12: NIST RISK MANAGEMENT FRAMEWORK (RMF) 45
FIGURE 13: NIST RMF HIERARCHY 48
FIGURE 14: NIST RISK ASSESSMENT PROCESS 50
FIGURE 15: FAIR RISK MODEL 52
FIGURE 16: OCTAVE FRAMEWORK WORKFLOW 53
FIGURE 17: TARA METHODOLOGY 54
FIGURE 18: RISK MANAGEMENT LIFECYCLE. (BY TARI SCHREIDER, LICENSED UNDER A CREATIVE COMMONS 56
FIGURE 19: TOP 10 27001 CERTIFICATIONS BY COUNTRY 70
FIGURE 20: NIST CYBERSECURITY FRAMEWORK 72
FIGURE 21: CONTROL LIFECYCLE MANAGEMENT 73
FIGURE 22: CIA TRIAD: CIA TRIAD 75
FIGURE 23: PDC DEFENSE-IN-DEPTH MODEL 75
FIGURE 24: P6 CONTROL MATURITY MODEL (BY TARI SCHREIDER, LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION-NONCOMMERCIAL-NO DERIVATIVES 4.0 INTERNATIONAL LICENSE) 80
FIGURE 25: COMPLIANCE MANAGEMENT REFERENCE MODEL 84
FIGURE 26: INFORMATION SECURITY-RELATED ISO STANDARDS 89
FIGURE 27: NIST INFORMATION SECURITY-RELATED SPECIAL PUBLICATIONS 95
FIGURE 28: OWASP TOP 10 FOUR-YEAR VIEW 100
FIGURE 29: AUDIT PROCESS FLOW 107
FIGURE 30: RBIA PHASE 110
FIGURE 31: INFORMATION SECURITY PROGRAM CHARTER MODEL 117
FIGURE 32: STRATEGIC PLAN DEVELOPMENT LIFE CYCLE 121
FIGURE 33: 2017 HIMSS CYBERSECURITY SURVEY—STAFFING RATIOS 127
FIGURE 34: INFORMATION SECURITY PROGRAM ROADMAP 132
FIGURE 35: PROJECT MANAGEMENT LIFE CYCLE 133
FIGURE 36: PROJECT STAKEHOLDERS 134
FIGURE 37: ISO CONTINUITY OF OPERATIONS STANDARDS 136
FIGURE 38: DIGITAL FORENSICS FRAMEWORK 145
FIGURE 39: SECOPS FRAMEWORK 148
FIGURE 40: EVENT MANAGEMENT MODEL 151
FIGURE 41: INCIDENT RESPONSE MODEL 153
FIGURE 42: THREAT MANAGEMENT MODEL 156
FIGURE 43: PENETRATION TESTING OPTIONS 161
FIGURE 44: TESTING TEAM INTERRELATIONSHIP MODEL 161
FIGURE 45: SQRRL (AMAZON) THREAT HUNTING LOOP 164
FIGURE 46: AAA MODEL 168

nide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 47: ACCESS ADMINISTRATION LIFECYCLE 176
FIGURE 48: UPTIME INSTITUTE DATA CENTER TIER CLASSIFICATIONS 181
FIGURE 49: ISO NETWORK SECURITY STANDARDS 184
FIGURE 50: OSI MODEL 187
FIGURE 51: SECURE SDLC MODEL 200
FIGURE 52: DEVSECOPS FACTORY MODEL™ (BY TARI SCHREIDER, LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION-NON- COMMERCIAL-NODERIVITIVES 4.0 INTERNATIONAL LICENSE) 202
FIGURE 53: SECURE WATERFALL DIAGRAM 203
FIGURE 54: AGILE SECURITY MODEL 204
FIGURE 55: VIRTUALIZED ENVIRONMENT 214
FIGURE 56: NIST SP VIRTUALIZATION PROTECTION GUIDANCE 217
FIGURE 57: VIRTUALIZED SECURITY REFERENCE MODEL 218
FIGURE 58: CLOUD COMPUTING TYPES 219
FIGURE 59: INFORMATION SECURITY PROGRAM SUPPORT PYRAMID 233
FIGURE 60: STRATEGIC INFORMATION SECURITY PLAN FRAMEWORK 236
FIGURE 61: GOALS ALIGNMENT RELATIONSHIP MODEL 237
FIGURE 62: TACTICAL TIME-BOUND GOAL OVERVIEW 238
FIGURE 63: INFORMATION SECURITY STRATEGY COMMUNICATIONS PLAN 239
FIGURE 64: CYBERSECURITY PROGRAM BLUEPRINT. (BY TARI SCHREIDER, LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION- NONCOMMERCIAL-NODERIVATIVES 4.0 INTERNATIONAL LICENSE) 241
FIGURE 65: CYBERSECURITY ARCHITECTURE SCHEMA (CAS)™. (BY TARI SCHREIDER, LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION-NONCOMMERCIAL-NODERIVATIVES 4.0 INTERNATIONAL LICENSE) 242
FIGURE 66: INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) STRATEGY 245
FIGURE 67: INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) CONTINUOUS IMPROVEMENT PROCESS (CIP) MODEL 246
FIGURE 68: ZACHMAN 6 X 6 MATRIX 249
FIGURE 69: STRUCTURE OF THE OPEN GROUP ARCHITECTURE FRAMEWORK (TOGAF) ARCHITECTURE 251
FIGURE 70: FEDERAL ENTERPRISE ARCHITECTURE FRAMEWORK (FEAF) 253
FIGURE 71: IT SPENDING AND STAFFING BENCHMARKS STUDY FOR 2022/2023 256
FIGURE 72: INFORMATION SECURITY SPENDING PERCENTAGE BY IT CATEGORY 261
FIGURE 73: VENDOR PROCUREMENT CYCLE 267

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

List of Tables

TABLE 1: REACTIVE VERSUS PROACTIVE ATTRIBUTES 5
TABLE 2: RISK ESSENTIALS PROGRAM CHECKLIST 22
TABLE 3: RISK ASSESSMENT TYPES 24
TABLE 4: ANNUALIZED LOSS EXPECTANCY MODEL 37
TABLE 5: RISK MANAGEMENT FRAMEWORKS 38
TABLE 6: RISK SCORE MATRIX 42
TABLE 7: ISO 27005 ANNEX C - EXAMPLES OF TYPICAL THREATS 60
TABLE 8: ISO 27005 ANNEX D - EXAMPLES OF VULNERABILITIES 62
TABLE 9: NIST SECURITY CONTROLS 77
TABLE 10: CONTROL CATALOG SOURCES CHART 80
TABLE 11: INFORMATION SECURITY SERVICE CATALOG EXAMPLE 82
TABLE 12: LEGAL TERMS DEFINITIONS 84
TABLE 13: LIST OF NERC CIP MANDATORY STANDARDS 93
TABLE 14: PCI DSS SECURITY REQUIREMENTS 94
TABLE 15: CIS CRITICAL SECURITY CONTROLS 100
TABLE 16: INTERNAL VS. EXTERNAL AUDIT FUNCTION COMPARISON CHART 105
TABLE 17: INTERNATIONAL AUDITING STANDARDS CHART 108
TABLE 18: SAMPLE STAKEHOLDER MANAGEMENT PLAN 121
TABLE 19: ALTERNATIVE RECOVERY SITE OVERVIEW 140
TABLE 20: EVENT CATEGORIZATION 153
TABLE 21: ACCESS CONTROL TYPE COMPARISON 175
TABLE 22: OSI MODEL MAPPED TO COUNTERMEASURES 188
TABLE 23: ENCRYPTION STANDARD COMPARISON 213
TABLE 24: CSA CORE VIRTUALIZATION RISKS 216
TABLE 25: CCM CONTROLS MATRIX 222
TABLE 26: BUSINESS TO INFORMATION SECURITY GOALS ALIGNMENT EXAMPLE 232
TABLE 27: SABSA 6 X 6 MATRIX 252
TABLE 28: THIRD-PARTY ASSURANCE PROGRAM PROVIDERS 272

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.
hide01.ir

C|CISO

dc01.ir

DOMAIN 1

Governance & Risk Management (Policy, Legal & Compliance)

EC-Council

Governance

As the field of information security continues to mature, integration with the rest of the organization and the importance of partnering with executive leadership and the board of directors takes on even more importance. Implementing governance and risk management mechanisms within the information security function is more essential today than ever—it is foundational to business function and success.

A building requiring a stable foundation to support the construction, governance, and risk management constitutes the foundation a CISO must implement and maintain for a strong and healthy information security portfolio.

Knowledge Assumptions

The C|CISO Body of Knowledge (BOK) assumes a foundational understanding of governance, risk management, and compliance (GRC) concepts. GRC is a standard information security leadership concern. Still, a review of it begins with an evaluation of corporate governance as the foundation that defines the processes, structure, and tools used to direct and manage all activities of an organization. Information security is typically an integrated governance structure influencing the processes that produce the products and services delivered to the consumers and stakeholders of an organization.

hide01.ir

Definitions

Some definitions that will assist the reader throughout this domain are described in this section.

- **Governance**

  Information security governance is defined as establishing and maintaining a framework and supporting management structure and processes to ensure that information security strategies are aligned with and support business objectives. To manage risk, this governance structure is consistent with applicable laws and regulations, enables adherence to policies and internal controls, and assigns responsibility for secure operations.

  Simply put, information security governance is the active involvement of senior management in the institutionalization and oversight of the information security program for an organization.

- **Compliance**

  Compliance is the act of conforming to stated requirements. At an organizational level, it is achieved through management processes that identify the applicable requirements (defined, for example, in laws, regulations, contracts, strategies, and policies), assess the state of compliance, evaluate the risks and potential costs of noncompliance against the projected expenses to achieve compliance, and then prioritize, fund, and initiate necessary corrective actions.

- **Privacy**

  Privacy in the context of information security is ensuring that an individual's personal information is kept secret from others and companies with whom they do not wish to share their confidential information. Providing privacy is challenging today's instantaneous information sharing, social media, and big data. Information security managers can seek

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

guidance from one of the most pragmatic and straightforward definitions of privacy, provided by Brandeis and Samuel in three articles published in the Harvard Law Review between 1888 and 1890. This began a new chapter in US law and formed the basis of modern privacy.

- **Risk Management**

  Risk management is the set of processes through which management identifies, analyzes, and responds to threats that can adversely affect realizing the organization's business objectives. The response to associated risks typically depends on their perceived criticality and results in remediating, avoiding, accepting, or transferring risk to a third party.

1. DEFINE, IMPLEMENT, MANAGE, AND MAINTAIN AN INFORMATION SECURITY GOVERNANCE PROGRAM

The corporate governance framework consists of explicit and implicit contracts between the company and the stakeholders to distribute responsibilities, rights, rewards, and procedures for reconciling the sometimes conflicting interests of stakeholders. Fulfilling the governance framework is done by stakeholder duties, privileges, roles, and strategies for proper supervision (as well as control and information flows) to serve as a system of checks and balances [1]. Reconciling the conflicting interests of stakeholders requires an understanding of the drivers that influence these interests.

A business driver is a condition, process, requirement, or other concern influencing how an organization directs or manages its activities. A close relationship exists between the drivers affecting an organization and the governance processes established to manage activities. At the highest management levels, corporate governance defines how the organization will achieve its mission, vision, and objective. The CISO must understand why an organization exists and how it conducts business before the development of information security governance can begin.

Governance provides a structure to support the delivery of results that satisfy the interests and objectives of stakeholders, regardless of whether those stakeholders are shareholders, investors, employees, suppliers, customers, or the community. The form of business organization, its hierarchical structure, the industry in which it operates, and its maturity all work together to influence the product of corporate governance in an organization.

1.1. Form of Business Organization

The organization's structure creates vital considerations when determining how the organization functions.

Proprietorships, partnerships, and corporations are the three most common business organizational structures. Each structure uniquely influences the scope and complexity of governance within an organization.

As an organization increases in size and complexity, the number of stakeholders and their competing interests also grows. These factors define the form of corporate governance that best enables an organization.

A proprietorship, the simplest form of ownership, exists when a single individual owns the organization, receives all the benefits of its operation, and assumes responsibility for its liabilities. The proprietor defines the organization's mission, vision, and purpose based on their experience

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and priorities. The power to make decisions rests solely with this person.

A partnership (like a proprietorship) consists of two or more individuals who share the benefits and the responsibilities for the operational viability of the organization. Partnerships allow owners to pool their knowledge and experience. However, governance becomes more complex as the partnership works to address the perspectives and desires of additional vested owners.

A corporation is the most complex form of business. Corporations exist as legal entities that are separate from their owners. Governance is a directed activity because owners must establish the rules for running the corporation within the articles of incorporation. Shareholder value is the primary focus of governance within corporations. That value can exist as a financial return or as a product or service delivered in the community's interests, representing the greater good.

1.2. Industry

The industry in which an organization operates affects corporate governance. A limited set of enterprises is the subject of most discussions about governance due to typical media percentage coverage, including public, retail, information, and financial services. However, various industries exist, and each has specific concerns and industry-specific requirements that drive governance decisions. The drivers applied within a particular sector rarely affect other industries similarly. Unique business drivers affecting each industry require tailored approaches to manage industry-specific concerns. For example, problems regarding Protected Health Information (PHI), contracted providers, and data sharing in healthcare organizations are entirely different from those of retail, agriculture, manufacturing, or financial services organizations, which all have other operational models and business drivers.

hade01.ir

1.3. Organizational Maturity

The maturity of an organization influences governance. Maturity varies irrespective of the size of an organization, or the structure established to manage its activities. The concept of maturity maps to the Capability Maturity Model Integration (CMMI), a process model that defines what an organization should do to promote behaviors that facilitate improved performance levels.

LEVEL 1 Initial	**LEVEL 2** Managed	**LEVEL 3** Defined	**LEVEL 4** Quantitatively Managed	**LEVEL 5** Optimizing
Processes are unpredictable, poorly controlled, & reactive.	Processes are characterized for projects but is often reactive.	Processes are characterized throughout the organization & proactive. (Projects map their processes to organizational standards)	Processes are measured & controlled - proactive.	Focuses on process, improvement, & enhancing existing processes.

Figure 1: CMMI Model Outline

Most organizations begin as immature and reactive, whether a proprietorship, a partnership, or a corporation. Here, processes could be more predictable, better controlled, and sensitive. As they mature, organizations define strategies and move toward increasingly proactive and formalized policies, procedures, and methods that improve performance across individual business practices or the entire enterprise.

The effectiveness of governance varies as organizations move from immaturity to maturity along the CMMI model. Defining formal processes is complex at Level 1 and Level 2, and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

methods are unpredictable or reactive. Organizations can only realize the benefits of mapping processes to organizational standards and achieving consistency across the enterprise once they attain CMMI Level 3. Achieving this level of maturity is essential for information security leadership because the CISO can only begin to establish formal standards for information security governance once the processes are classified throughout the organization.

Reactive	Attribute	Initiative-taking
Making money and short-term shareholder returns	Focus	Long-term returns and strategic directions
Reacting to immediate problems	Priorities	Taking a preemptive approach
Control is centralized	Control	Control is localized
Reliance on instinct or the experience of one or more people	Analysis	Focus on data to improve processes
People counted as a cost	Personnel	People are valued as an asset
Training is a benefit or reward	Training	Training is essential to success
Distrust between management and employees	Leadership	Leaders and personnel collaborate and work together

Table 1: Reactive versus Proactive Attributes

Some organizations take the steps necessary to achieve the highest level of maturity defined by CMMI Level 5; however, achieving and maintaining this degree of maturity is challenging and rare. Most organizations are satisfied with maturity Level 3 or Level 4 and focus on maintaining operations at this level because the cost and effort required to maintain CMMI Level 5 may not be worth the benefit of doing so.

Maturity affects an organization at the macro level and influences the micro level, where a mix of maturity can exist in different departments and business units across the organization. For example, Human Resources and accounting functions typically have higher maturity levels because of the established processes and procedures inherent in these business operations. Similarly, IT programs that follow the IT governance and service delivery models offered by Control Objectives for Information and Related Technologies (COBIT) or Information Technology Infrastructure Library (ITIL) are more likely to operate with higher maturity than organizations that do not use these types of formal standards to manage IT governance and IT service delivery.

2. INFORMATION SECURITY DRIVERS

Business drivers affect the decisions made within an organization. Information security drivers are also worth consideration because of their effect on the management and operation of a security organization. Alignment with the business, compliance, and privacy are typically the most essential information security drivers within an organization.

Corporate governance influences the programs and activities created to support information security governance. Priorities defined at the corporate governance level provide the foundation for most information security decisions. They often influence, and sometimes outweigh, information security priorities. Business and operational priorities of the organization affect not only the strategy for

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information security governance but also the resources dedicated to accomplishing security goals and objectives.

Organizational alignment is one of the most critical drivers for information security governance. The CISO can achieve harmony and alignment between the business and security by mapping information security governance to the foundations provided by corporate management. The success and effectiveness of this approach relies on understanding the influence of corporate governance and then incorporating corporate governance principles into the security program. Achieving this balance depends on the importance of executive buy-in and corporate communication. This effort will also highlight the value of relationships between the CISO and other organizational leaders. Optimally, information security governance should flow naturally from the highest levels of leadership and permeate, top-down, throughout the rest of the organization.

The approach used to achieve alignment with the business varies according to the organization's size, industry, and complexity. For example, larger corporations operating in regulated environments often dedicate more resources to a more comprehensive security program. Smaller organizations with fewer security resources tend to focus on critical components of the security program, saving organizational resources on the most important aspects of security and outsourcing other security program elements to vendors and managed service providers.

The CISO must understand the organization before alignment can occur. Because internal competitive forces produce different reactions to business drivers, the CISO must understand the objectives of the business, the business processes created to support those objectives, the information and technology supporting these processes, and the threats that could disrupt those processes.

iii0601.ir

3. ESTABLISHING AN INFORMATION SECURITY MANAGEMENT STRUCTURE

3.1. Organizational Structure

The hierarchical structure of an organization is closely related to its form of business organization. For example, the proprietorship's owner often acts as the CEO, and the organizational chart expands from this central figure to satisfy the owner's interests. Alternatively, partnership organizational charts are based on the experience and capabilities of partners. Power can rest with a single decision-maker or a committee. Corporations often have complex hierarchies and reporting structures. The CEO manages the corporation's daily operations but reports to a Board of Directors that provides oversight and direction for maximizing shareholder value.

3.2. Where does the CISO fit within the organizational structure?

No standard establishes the optimal placement of a CISO within the organizational hierarchy. Many variations exist depending on the type of organization and the industry in which it operates. An organization's structure, priorities, and the perspectives of its leaders primarily influence where the role exists. Placement decisions should focus on the objectives of the organization and the contribution that security makes in support of those objectives. This is superior to choosing placement based on industry assumptions or recommendations unrelated to the organization's needs.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

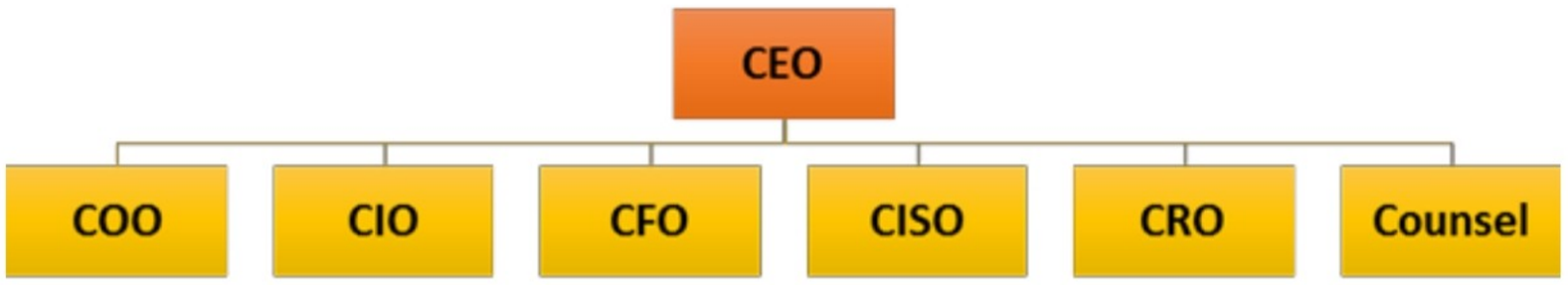


Figure 2: Organizational Structure

The CISO's placement in the organization is essential from all governance perspectives. An organization does not require the CISO to operate as a corporate executive to achieve success; however, the CISO should be positioned to have the necessary power and influence to lead and direct all information security governance activities.

3.3. The Executive CISO

CISOs who provide leadership as corporate executives are typically more effective because they have the advantage of influence and a voice equal to other organizational leaders. This positioning can increase awareness about information security concerns. The positioning also increases opportunities to provide top-down direction for incorporating security into the practices and culture of the organization.

Becoming an effective corporate executive requires significant business experience to influence the day-to-day leadership of an organization. This experience is different from the experience and training of most CISOs. Whereas most nontechnical executives receive training focused on organizational leadership, most CISOs have a history of leadership focused on technology solutions and other nonbusiness activities. Because of these differences in training and experience, many organizations limit the power and influence of the CISO exclusively to information security and technology-related risk management.

3.4. C-Level Attitudes toward the CISO

A survey of 200 C-suite-level executives by data security firm Threat Track found that 75 percent do not think the CISO should be part of the senior leadership team, even though 47 percent said the CISO should be held accountable if there is a breach. While CISOs are widely viewed as a valuable addition to corporate boards of directors, C-level executives still need to be convinced about their leadership abilities and understanding of business objectives outside of security [2].

The attitudes revealed in the Threat Track survey demonstrate a conflict of views regarding a CISO's perceived accountability for a breach and the power the CISO must have to prevent a violation by leading risk management efforts as part of the senior leadership team. Many executives expect accountability for a breach from the CISO. Yet, they have limited faith in the CISO's leadership abilities and the contribution this role can make to support positive results for both business and security objectives.

3.5. Nonexecutive CISO

The current most common placement of the CISO is a non-executive leadership role focusing on information security and risk management objectives rather than directing an organization's business activities. Although the CISO does not require executive status to support effective information security governance, appropriate positioning is needed. An organization should avoid placing the CISO within the hierarchy where competing interests exist, or the role has limited influence.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The unique objectives of an individual organization, the role security plays in supporting those objectives, and the perspective of organizational leaders help to determine the optimal placement of the CISO within the hierarchy. For example, the CISO may report to the Chief Information Officer (CIO) when it prioritizes innovation, information management, and IT service delivery. Within this structure, the CISO may focus on incorporating security practices into organizational technology and IT services. The CISO may report to the Chief Risk Officer (CRO) in regulated industries that require a CRO to manage enterprise risk management (ERM), which encompasses a variety of risks beyond information security. In this model, the CISO works and reports information security risks as a peer to business leaders in other risk areas of the organization. The CISO may report to the general counsel in organizations that focus on risk management from a legal perspective. This model leads the CISO to collaborate closely with the legal team and contribute to third-party risk management, contract security, and other risk areas overseen by the general counsel.

4. LAWS/REGULATIONS/STANDARDS AS DRIVERS OF ORGANIZATIONAL

4.1. POLICY/STANDARDS/PROCEDURES

Many of the activities of a CISO involve dealing with laws, regulations, and standards. These drive the development of an organization's information security policies, standards, and procedures. Information security analysts have often said that GRC may account for half of a CISO's time. This is easy to understand when considering the myriad laws, regulations, and standards an organization must comply with. CISOs today need to spend time reviewing and staying informed of proposed and enacted changes to anything that is potentially affected by the GRC activities of their information security program.

Regulations are written laws passed by a legislative body or enabled by an executive body through the interpretation of laws passed by a legislative body. Laws outline the principles and regulations established in a community by some authority that apply to its people, whether in the form of legislation or customs and policies recognized and enforced by a judicial decision [3]. Organizations must comply with requirements documented in the jurisdiction where a particular law was passed.

Standards are created by various third-party organizations and are designed to provide a framework to assist organizations in building their information security program by following principles often developed by the information security community. They do not hold the same weight as laws/regulations; however, they often include significantly more detailed advice regarding implementing the security program.

The policies, standards, and procedures created by an organization reflect a combination of regulatory/legal directives, third-party measures, and risk-based considerations that reflect the organization's risk appetite (the level of risk an organization is willing to accept).

Domain 2 describes the most common laws, regulations, and standards a CISO can encounter.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. MANAGING AN ENTERPRISE INFORMATION SECURITY COMPLIANCE PROGRAM

Organizing the information security program requires compliance with various laws, regulations, standards, and frameworks. The practical mechanism for enabling this activity is creating an information security management program.

Information security management programs are comprised of more than just firewalls and passwords. They are organization-wide programs designed to enable the business to operate at reduced risk.

The effective management of information security in an organization or enterprise encompasses all organizational and operational processes and participants relevant to information security.

Information security should be an ongoing process, which, when fully developed, will position an organization to manage the most critical security issues so that the business can fulfill its objectives.

The information security management framework is a combination of well-defined policies, processes, procedures, standards, and guidelines for establishing the required level of information security. The following shows how the individual parts of a comprehensive information security management system fit together.

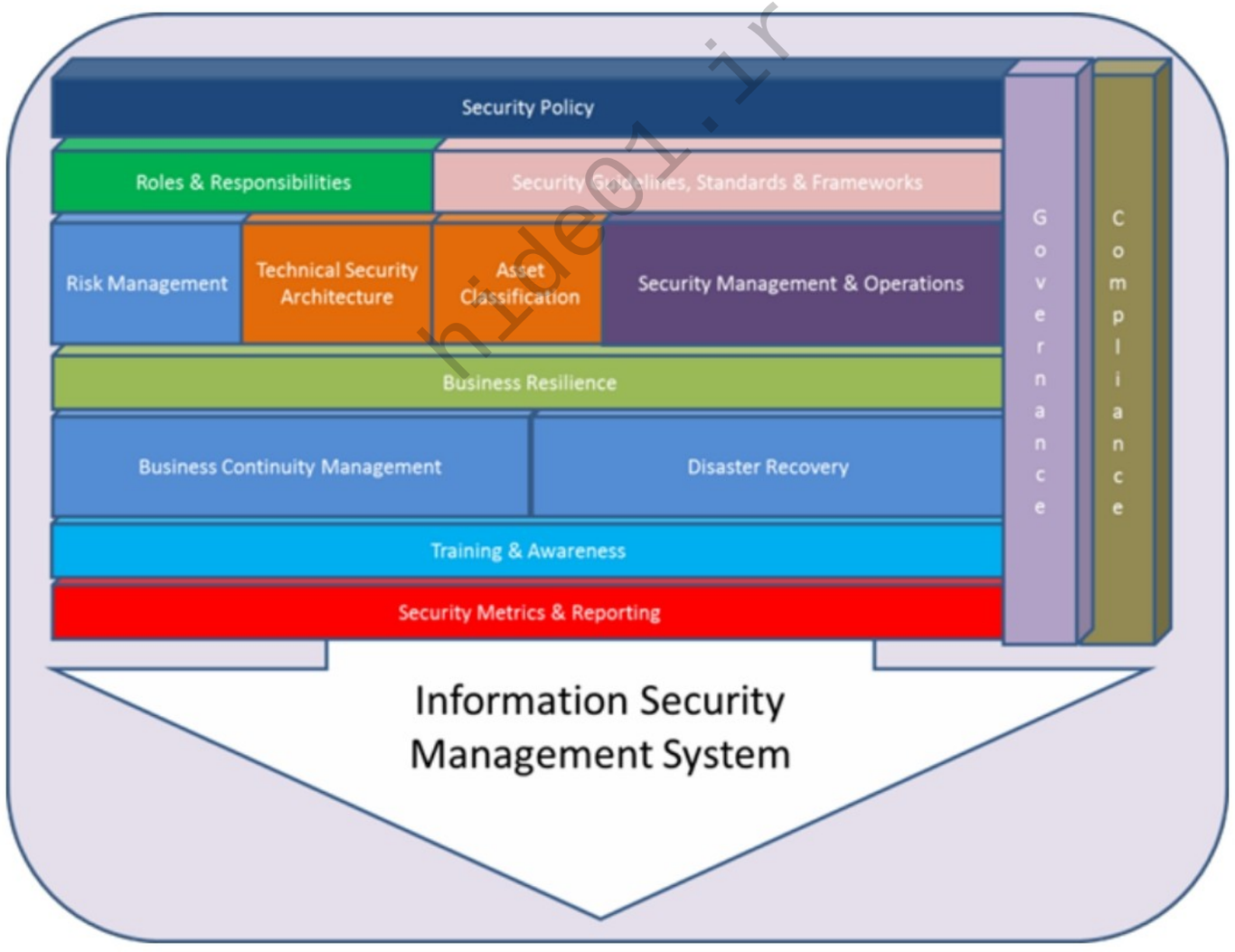


Figure 3: Information Security Management System/Framework

5.1. Security Policy

Security policies are governance direction documents revolving around "shall/shall not," "will," and "must" statements for specific organizational focus areas. Governance, risk, compliance, privacy, and security staff often create these documents, and they include higher-level language dictating "who," "what," "why," "when," and "where." Supporting policies (e.g., IT asset inventory) may supplement primary security policies (e.g., IT asset categorization).

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security policies aim to provide vendor- and technology-agnostic direction, which may include both general and specific directives. Still, they usually do not contain detailed steps describing "how" security controls should be implemented. Security policies are abbreviated "business plans" illustrating strategically mandated security principles to mitigate organizational risk, protect the confidentiality, integrity, and availability (CIA) of information assets, and promote business resiliency. These documents must also comply with applicable laws and regulations, providing sufficient clarity for proper application by the reader.

A security policy should be clear, concise, consistent, and easily understood by the target audience (clearly identified in the document), without an abundance of confusing or obscure language (e.g., undefined acronyms, technical jargon, or complicated legal terms). Often, the writer will use an organizational standard policy template or leverage and update a previously created document.

When creating a new policy or updating an existing one, the author should endeavor to avoid and remove any language leading to a potential misunderstanding. Quality is more important than quantity or length, and a professionally designed and planned policy integrates well within existing business structures or fortifies new ones, facilitating endorsement and adoption. All organizational policies should align with organizational priorities and executive-level security expectations.

A primary security policy typically includes the following:

- The extent to which everyone in the organization has a stake in information security
- The confidentiality and privacy of information
- The principle of least access to information
- The integrity of information
- The availability of information
- The balance of risk exposure with the cost of risk mitigation
- The implementation of security measures
- The classification of information
- The importance of security awareness and information governance

ride01.ir

Many of these principles are common across most major security regulations and standards. These principles are consistent with accepted and proven industry best practices for security management.

5.1.1. Necessity of a Security Policy

It is only possible to accomplish a complex task with a detailed plan. A security policy is a plan that provides for consistently applying security principles throughout your company. After implementation, it becomes a reference guide for matters of security. A security policy indicates senior management's commitment to maintaining a secure environment, which allows the IT staff to be more effective in securing the company's information assets. A security policy will reduce the risk or limit security incident damage. In the event of a security incident, specific policies, such as an incident response policy, may limit your company's exposure and reduce the severity of the incident.

A professionally written security policy can help legally protect an organization because it demonstrates its commitment to legal and regulatory requirements. Security policies specify

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

how users can and cannot use IT resources, how they should maintain the privacy of confidential information, and how to protect data adequately, reducing liability and exposure in the event of an incident. A security policy also provides a written record of a company's intent if there is a question about what is and is not an approved act. Third parties that do business with a company often require security policies as part of due diligence. Some examples include auditors, customers, partners, and investors. Companies that do business with your company, particularly those sharing confidential data or connectivity to electronic systems, will be concerned about your security policy. Finally, one of the most common reasons companies create security policies is to fulfill regulations and meet standards related to digital information security.

Finally, one of the most common reasons companies create security policies is to fulfill regulations and meet standards related to digital information security. A few of the more common ones include:

- The Payment Card Industry (PCI) Data Security Standard (DSS)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Health Information Technology for Economic and Clinical Health (HITECH) Act
- The Sarbanes-Oxley Act (SOX)
- Massachusetts 201 CMR 17.00
- The ISO family of security standards
- The Gramm–Leach–Bliley Act (GLBA)
- The EU General Data Protection Regulation (GDPR)

hideol.ir

5.1.2. Security Policy Challenges

Security, compliance, and privacy policies take work to create. Writing a policy is complex and time-consuming due to the need to be endorsed and adopted within the organization. To be effective, a security policy must be clear and consistent. A security policy should fit within existing business structures and not mandate a complete, ground-up change to how the business operates.

5.2. Policy Content

A security policy must be so written that it can be understood by its target audience (which should be identified in the document). For example, technical policies are written for the intended audience. Higher-level policies should be written in commonly understood language. A security policy should not use confusing or obscure language, such as jargon or uncommon legal terms.

The goal of policies is quality, not quantity. One page of concise information is far better than 100 pages of impressive-looking details if one page contains actionable items contributing to the overall information security plan.

A security policy should not allow for the potential for misunderstanding. There must be a universal comprehension of the policy and consistent application of security principles across the company.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A typical structure for a security policy consists of the following sections:

- **Overview:** provides background information on the issue that the policy will address
- **Purpose:** specifies why the policy is needed
- **Scope:** defines precisely who and what the policy covers
- **Target audience:** advises those individuals to which the policy is intended
- **Policies:** this is the main section of the document and provides statements on each aspect of the policy. For example, an acceptable use policy might have individual policy statements related to internet use, email use, software installation, and network access from home computers.
- **Definitions:** technical terms or acronyms are defined
- **Version:** to ensure consistent use and application of the policy, versioning is used to indicate changes and updates to the policy

A security policy should be as long as necessary. Some security professionals believe policies are more impressive when they fill enormous binders or contain numerous policies. This approach overwhelms users and departments and needs to be more frequently addressed. These are the types of policies that become "shelfware."

A security policy should be written in plain language. Technical topics should be clear and easily understood by the target audience for that policy. Policies should be written so that more people can understand them rather than fewer. Clarity is always a priority in security policies so that a policy is correctly understood, which could lead to organizational risk exposure.

A security policy must be consistent with applicable laws and regulations. In some countries, some laws apply to a company's security practices, such as using encryption. Some states have specific disclosure laws or regulations governing the protection of personal information, and some industries have regulations governing security policies. You should research and become familiar with all regulations or standards affecting your company's security controls.

A security policy should be reasonable. Creating an effective policy is to secure the organization rather than make your company appear secure, but it is impossible to ensure due to poorly written policies. Remember that the more security a policy specifies, the greater the compliance burden it places on users and IT staff. Find a balance between security and usability that reflects the overall risk tolerance of the organization.

A security policy must be enforceable. A policy should clearly state what actions are permitted and violate the policy. Further, the policy should determine enforcement options when noncompliance or violations are discovered. These potential actions must be consistent with applicable laws. A security policy can be formatted to be compatible with your company's internal documentation; however, certain information should be placed on each policy page. This information should include the policy name, creation date, and specific target audience.

5.2.1. Types of Policies

Some organizations will need additional policies for effective security management. Some standard policies that could make up an organization's security policy are listed below. Some companies may need all those listed, while others might need only a few. How many of these policies are used will depend upon the framework or frameworks the organization follows. A

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

healthcare organization may choose to organize the set of policies to closely align with the Health Information Trust Alliance (HITRUST) requirements. In contrast, an international manufacturing company might prefer to align its policies according to ISO 27001 requirements. The mechanism for arranging and aligning the policies to a framework should be based on organizational needs.

Specific policies are essential to fundamental security management and apply to many organizations. These are denoted in the following list with an asterisk.

- Acceptable Use Policy*
- Application Security Policy*
- Asset Management Policy*
- Backup Policy*
- Business Continuity/Disaster Recovery Policy*
- Confidential Data Policy*
- Data Classification Policy*
- Data Retention Policy*
- Encryption Policy*
- Email Policy*
- Identity and Access Management (IAM) Policy*
- Incident Response Policy*
- Mobile Device Policy*
- Network Access Policy*
- Network Security Policy*
- Outsourcing Policy
- Password Policy*
- Physical Security Policy
- Remote Access Policy
- Third-Party Management Policy*
- Threat and Vulnerability Management Policy*
- Wireless Access Policy

hide01.ir

5.2.2. Policy Implementation

Once the security policy has been created, deploying it throughout an organization is the most challenging part of the process. Too many well-intentioned projects lose initiative in this phase, so this step must be well-planned and thoughtfully implemented.

The organization's senior management team must back a security policy. Without such support, the cooperation needed across departments will impair or halt policy implementation.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Department leads and other stakeholders must be involved in the effort. Other critical support functions include human resources, legal services, and internal audit. Management buy-in is needed before the implementation process moves forward.

If the position does not exist, an information security officer or program manager should be designated at the organization. This position is responsible for implementing and managing the security policy. An existing manager can fulfill this position. This designation is sometimes not practical for smaller companies. Still, regardless, one person with the authority to make executive decisions must own and be accountable for an organization's security policy.

Remember that a security policy must be officially adopted as a standard company policy. It should be approved and recorded like an organization makes other significant decisions, including full senior management approval.

Review each policy and consider its application within the organization if policies already exist. Make sure that the tools exist to support conformity with the policy. For example, if the policy specifies that a specific network must be monitored, ensure that specified monitoring capabilities can be applied to that network segment. If a policy sets that visitors must agree to the acceptable use policy before using the network, ensure this policy is implementable from a people, process, and/or technology perspective. If you discover something impractical, create a plan to make appropriate changes to enable adherence or modify the policy.

Understand that policies differ from processes and procedures. You must carefully consider the supporting security processes and procedures as the policy is created. For example, a backup policy may detail the requirement for schedules for backups and off-site rotation of backup media; however, it will not provide how these tasks will be procedurally accomplished.

Additionally, standards and procedures must be created to support the policies. For example, how should your users respond if they suspect a security incident? How will you notify your users if they are non-compliant with a specific policy? How will exemptions to the policy be requested and approved? CISOs must work with the organizational structure (Legal, IT, HR etc.) to establish support for policies.

User education is critical to a successful security policy implementation. A training session should be held to review the policies impacting users and provide basic information security awareness training. Often, users create security issues because they don't understand that what they are doing is risky or contradictory to the security policy.

5.2.3. Security Roles and Responsibilities

The structure of the security team will vary based on the size of the organization, the industry in which the organization operates, and the regulatory landscape in which the organization operates. Other factors include budget and organizational maturity.

What all organizations have in common from the perspective of a security function is that one individual must have overall responsibility for the implementation and success of the security program.

Traditionally, the role of the CISO has been to develop, implement, and maintain processes across the enterprise with the following objectives:

- Reduce risks in the IT environment
- Establish and enforce security policies and procedures

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Establish security standards and controls
- Respond to cyber incidents

Over the last several years, necessity and opportunity have added essential responsibilities to the CISO's role in today's enterprises. These can include direct or shared responsibilities such as:

- Information risk management—determining risk factors and solutions
- Privacy
- Law enforcement agency interaction
- Balancing security needs with the company's strategic business plan
- Developing security policies and procedures that provide business protection
- Information security architecture
- Information security assurance
- Identity and access management
- Information regulatory compliance (for example, US PCI DSS, FISMA, GLBA, HIPAA; UK Data Protection Act 1998; Canada PIPEDA)
- Information technology controls for systems
- Computer Emergency Response Team/Computer Security Incident Response Team (CERT/CSIRT)
- Planning and testing responses to security breaches
- Searching for the sources of network attacks and information theft
- IT investigations, digital forensics, eDiscovery, fraud
- Disaster Recovery and Business Continuity Planning (DR/BCP)
- Information Security Operations Center (ISOC) implementations

hide01.ir

The ideal CISO must assume a business leadership position and dispel the idea that information security is a technology issue. They must encompass education and cultural change beyond security technology and processes. Leaders must reorient their enterprises to focus on initiative-taking risk management rather than crisis response and compliance. Information security management must migrate from discrete, fragmented initiatives to an integrated, systemic approach.

A CISO is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets are adequately protected. The CISO directs staff in identifying, developing, implementing, and maintaining processes across the organization to reduce information and IT risks, respond to incidents, establish practical standards and controls, and direct the establishment and implementation of policies and procedures. In addition to the above, the CISO is also responsible for information security compliance.

Having a CISO or the equivalent function in the organization has become a standard in most business, government, and nonprofit sectors. Throughout the world, a growing number of organizations have a CISO.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5.3. Reporting Structure

It is repeatedly asked in all industries: to whom should the CISO report? The vast majority of CISOs either report to or are in the reporting structure of the CIO. While this is the most common reporting structure, arguments can be made that this may be the most ineffective place in the organization for the CISO to report. The reason for this is the immediate conflict of interest that is potentially created by having the person responsible for assuring the confidentiality, availability, and integrity of information technology assets report to the individual who manages those assets and is often responsible for implementing security controls.

Many dependencies and variables will determine whether a given organizational security structure will succeed, and it can be complicated. There are numerous instances of CISOs reporting to the Chief Financial Officer (CFO), general counsel, and even directly to the Chief Executive Officer (CEO). Data indicates that none of these reporting structures have produced security programs vastly superior to others. Each case has different challenges and dynamics based on the type of business, the personalities involved, and many other factors. Each organizational structure has advantages and disadvantages, which are difficult to quantify. There is no correct answer regarding where a CISO should report.

Should the position even be called CISO? Some organizations have consolidated security, privacy, and compliance, all under the leadership of a senior executive named Chief Risk Officer (CRO). This approach has its advantages and disadvantages, as does any organizational structure. This structure decouples and distances the security organization further from the IT organization, which can cause some concerns. Others find this distancing more effective, allowing for a better separation of duties. Another possibility is that of a compliance organization consisting of internal auditors and some security technology experts whose primary responsibility is to interpret the technology for the auditors.

hideo1.ir

Regardless of structure, CISOs must ensure that technology solutions are more than just compliance items supporting an audit. They need to validate that solutions perform a necessary function and do not exist for the sole benefit of an audit. This approach assumes that enough technically astute support resources are available to implement the technology while providing compliance.

A critical element for the CISO to achieve maximum effectiveness is to have authority within the organization. This means the CISO must have visibility and respect from other senior executives. A CISO must be viewed as an executive peer, not just a technical individual. The CISO must have a clear view of and understand the company's broader business goals.

Without having the proverbial "seat at the table" with other business executives in a forum, it is unlikely that information security risk will be properly managed and will get properly integrated into the business processes.

5.4. Standards and Best Practices

Earlier in this chapter, it was noted that an organization can align to various standards. It was also pointed out that organizations should choose criteria and practices that most closely align with organizational requirements specific to the industry and the legal/regulatory frameworks that an organization must adhere to. It is critically important that the CISO lead the organization through determining what is required and how to best comply with these requirements.

There are a variety of standards and leading practices precisely because there are a variety of

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

organizations. When one approach might be appropriate for a healthcare company focused on maintaining patient privacy, that practice may not be suitable for a social network company that shares personal information between customers.

If you are the first CISO at an organization, choosing standards, frameworks, and creating best practices for your security function will be required. Luckily there are myriad resources available to help. You will likely have to employ a combination of utilizing existing tools, customizing them as needed, creating new content, and integrating them with your understanding of the organization.

A governmental organization or an organization that exclusively does business with a government entity would choose to align with a governmental information security standard. In the United States, it would most likely be the NIST Cyber Security Framework (CSF) and SP 800-53; thus, the CISO would build a security program that aligns with the CSF and NIST SP 800-53.

A healthcare CISO in the United States would most likely choose to align the security program to the HITRUST Common Security Framework (CSF). A healthcare company in the United Kingdom working with the National Health Service would most likely align with ISO 27001.

Your mission is quite different if you are a CISO entering a mature organization that has already aligned to a standard framework and created best practices for itself. You must understand the choices that were made. Based on your understanding of organizational direction and existing requirements, you would determine whether the choices made in the past are still valid. You would decide whether it is appropriate to change the security structure or retain the existing alignment.

The new or incoming CISO needs to spend time investigating options. Review available standards and frameworks to determine which will best align with your company's regulatory or industry requirements and suit the security program strategy and goals.

hidoot.ir

5.5. Leadership and Ethics

Leadership

A CISO needs to dynamically lead the information security function and clearly define what the security function should provide for the organization it supports. The CISO should also be a representative of the overall organizational leadership. The CISO must inspire the security team and IT system users to garner support.

Leadership is an intangible quality that requires more work to define. As CISO, you will be called to lead, inspire, and drive your organization to improve security effectiveness.

Laws, regulations, standards, frameworks, and internal policies, standards, and procedures are words on a page. They are guides for creating and documenting a program; however, the only way to make them effective is to lead your team and your organization into understanding and believing that information security is essential to the organization's success.

Being a successful leader is a journey, and being an effective leader in one organization does not ensure similar success in another.

Managers fill out paperwork, meet HR requirements, and/or assign tasks. Leaders have followers. Leaders are very often willing to do what they ask of their teams and members.

Ethics

Ethics define the moral principles that govern the behavior of a person or group. Appropriate and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ethical behavior is crucial for all activities the CISO conducts or directs within an organization. Because of the influence associated with the role of the CISO, the behavior of the CISO is evident and analyzed and often influences the character and behavior of other people throughout the organization. An unethical person in the CISO role can cause considerable damage to the image of an organization and the business it conducts.

CISOs often have significant access to sensitive information and systems within an organization. Only some people in an organization have the same access to knowledge and information as the CISO. Having solid ethics is critical.

A Seven-Question Framework for Ethical Decision-Making

All managers are typically trained to adhere to an organization's code of ethics. Most companies include this training as part of the corporate human resources processes for employee onboarding and have it in annual training. However, these codes of ethics are not always a good guide to ethical behavior. Part of the problem is that codes often specify what cannot be done rather than what should be done. And some codes focus more on ensuring that decisions are legal rather than correct.

The following framework for ethical decision-making consists of seven questions that, in answering, will serve as an aid to identify what is right.

When evaluating a decision, ask the following:

- What decision alternatives are available?
- What individuals or organizations have a stake in the outcome of my decision?
- Will any alternatives harm an individual or an organization?
- Which alternative will do the best with the least harm?
- Would someone I respect find any of the alternatives objectionable?

After deciding on a course of action, but before acting, ask the following:

- Am I comfortable with the decision I have made?
- Will I be comfortable telling my friends and family about this decision?

5.6. EC-Council Code of Ethics

EC-Council codifies the expectations for ethical behavior by certification holders within the EC-Council Code of Ethics [4]. This code provides a minimum standard of appropriate conduct at the CISO level and all levels of professionalism within the security industry. This code of ethics expresses the consensus of the profession on ethical issues. It is a means to educate the public and those entering the field about the ethical obligations of all e-commerce consultants. By joining the EC-Council, each member agrees to the following:

- Keep information within your professional work private and confidential.
- Protect intellectual property within your span of control.
- Disclose attacks and criminal activities to the appropriate persons or authorities.
- Provide the best service possible within your abilities as a security professional.
- Never knowingly use illegally or unethically obtained software or products.

hideo1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not engage in deceptive financial practices.
- Use the property of organizations as intended and authorized.
- Disclose potential conflicts of interest to all concerned parties when discovered.
- Provide good management and risk controls for projects you lead to deliver the highest quality product possible.
- Add to the profession's knowledge through personal knowledge improvement and sharing within the cybersecurity community.
- Conduct yourself most ethically and competently by never compromising your integrity.
- Do not associate with malicious entities or engage in malicious activities.
- Do not purposefully or intentionally expose or compromise an organization's systems or data.
- Ensure all systems scanning and penetration testing activities are authorized and performed within the applicable laws and statutes.
- Do not make inappropriate reference to the C|CISO (or any) certification, and never misuse your credentials or cause adverse perceptions to the C|CISO community.

6. INTRODUCTION TO RISK MANAGEMENT

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and impact [5]. Oversight for risk management is a critical activity that should occur within all organizations. Risk management begins at the corporate governance level of an organization, but the CISO has significant responsibilities concerning the implementation and execution of an organization's information risk management strategy.

Over the years, many risk management models have emerged from various organizations, including the Project Management Institute (PMI), the National Institute of Standards and Technology (NIST), insurance companies, and the International Standards Organization (ISO). The risk management methods, formulas, and outcomes vary whether the risk management process is in the context of project management, security, engineering, industrial functions, financial portfolio management, actuarial studies, or life safety. Regardless of the model selected, the CISO provides significant value by defining a structured and rigorous process to identify information security risks within an organization, proposing cost-effective treatment, and evaluating the performance of the selected treatment option.

Two essential risk concepts of risk management are:

Risk Appetite – How an organization addresses risk is primarily due to its risk appetite. You must determine if your organization has a large or small appetite for risk. The larger the appetite, the more likely an organization is to pursue higher-risk business activities.

Risk Tolerance – How much risk an organization is willing to accept in quantifiable terms is known as tolerance. Here, you need to determine the maximum amount of acceptable customer, financial, or reputational costs before acting or investing in risk mitigation.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.1. Risk Management Standards

The following is an overview of the five most popular risk standards referenced in creating risk management programs. The first set of standards comes from the National Institute of Standards (NIST) Special Publications (SP). The second set of standards are sourced from the International Standards Organization / International Electrotechnical Commission (ISO/IEC):

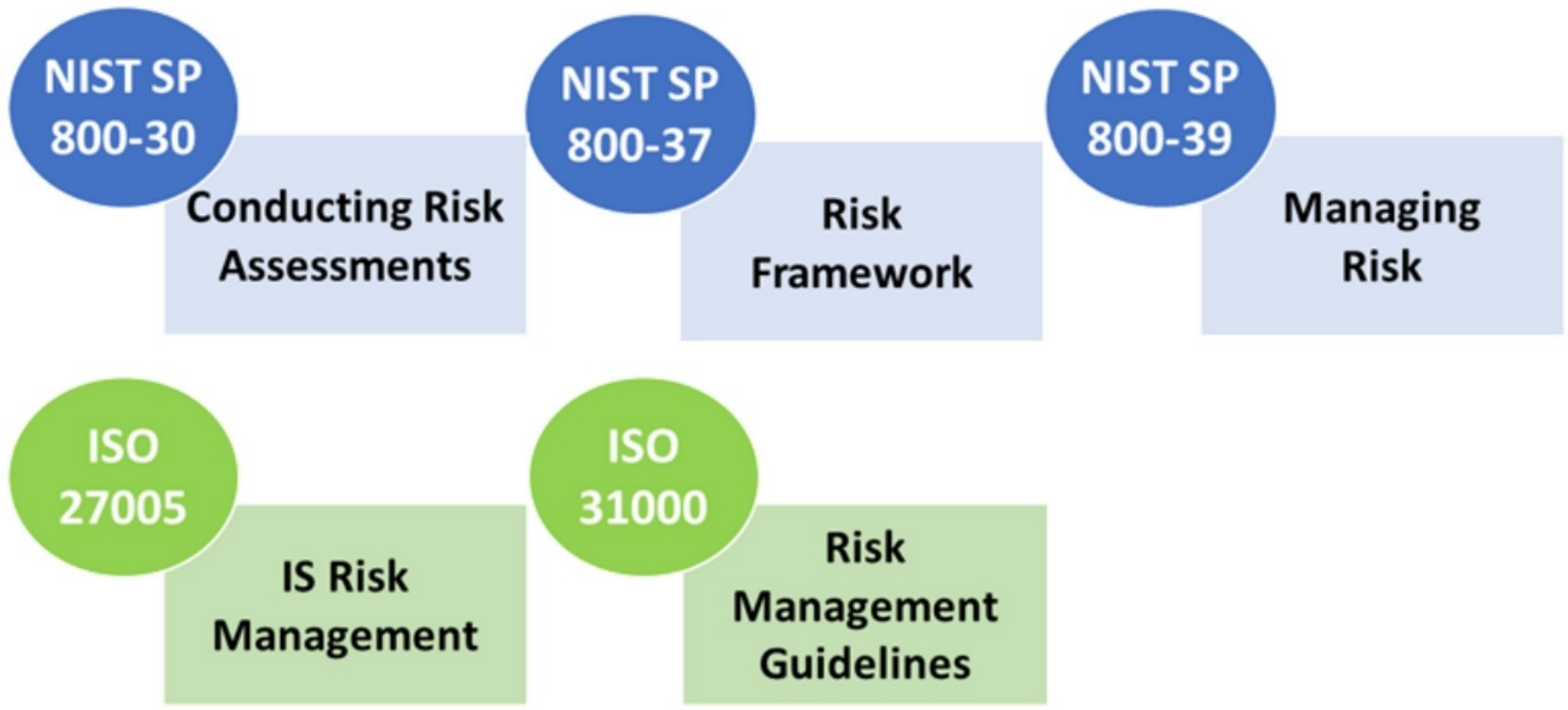


Figure 4: Risk Management Standards

NIST SP 800-30 Rev. 1 / Guide for Conducting Risk Assessments [6]

Special Publication 800-30 aims to guide conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments conducted at all three tiers (tier 1 organization, tier 2 mission/business/process, tier 3 information system) in the risk management hierarchy are part of an overall risk management process, providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

NIST SP 800-37 Rev. 2 / Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [7]

This publication provides guidelines for applying the Risk Management Framework (RMF) to information systems and organizations. The RMF includes:

- A disciplined, structured, and flexible process for organizational asset valuation.
- Control selection, implementation, and assessment.
- System and common control authorizations.
- Continuous monitoring.

It also includes activities to help prepare organizations to execute the RMF at the information system level.

The RMF promotes the concept of near real-time risk management and ongoing system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective risk management decisions about the systems supporting their missions and business functions; and integrates security and privacy into the system development life cycle [7].

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NIST SP 800-39 / Managing Information Security Risk: Organization, Mission, and Information System View [8]

The purpose of Special Publication 800-39 is to guide an integrated, organization-wide program for managing information security risks to organizational operations (that is, mission, functions, image, and reputation), corporate assets, individuals, other organizations, and the nation resulting from the process and use of federal information systems. Special Publication 800-39 provides a structured yet flexible approach for managing information security risks that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring threats on an ongoing basis provided by other supporting NIST security standards and guidelines.

The guidance provided in this publication is not intended to replace or subsume other risk-related activities, programs, processes, or approaches that organizations have implemented or plan to implement, addressing areas of risk management covered by other legislation, directives, policies, programmatic initiatives, or mission/business requirements. Instead, the information security risk management guidance described herein is complementary and can be used as part of a more comprehensive enterprise risk management (ERM) program.

The International Standards Organization / International Electrotechnical Commission (ISO/IEC) also publishes a set of standards on risk management guidance:

ISO/IEC 27005:2018 / Information technology -- Security techniques -- Information security risk management [9]**.**

This document provides guidelines for information security risk management.

It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is essential for a complete understanding of this document.

ISO/IEC 31000:2018 / Risk management – Guidelines, provides principles, framework, and a process for managing risk [10]**.**

This document can help organizations increase the likelihood of achieving objectives, improve identifying opportunities and threats, and effectively allocate and use resources for risk treatment.

Portions of these standards will be used throughout this book to illustrate the risk management process.

While not in the top five given their nascence (released in November 2023), the following NIST Special Publications are also worth noting.

NIST SP 800-221 / Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio

NIST SP 800-221A / Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio

6.2. The Essentials of a Risk Management Program

Regardless of which standard or framework is used to implement a risk management function, certain essential elements are shared among them. The following is a checklist that provides common elements that are defined or completed within a risk management program:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. Understand the context of which risk is to be evaluated.	✓
2. Create a risk management policy.	✓
3. Personalize risk management terms including risk appetite, risk tolerance, etc.	✓
4. Obtain executive buy-in on risk policy and terms.	✓
5. Understand and inventory the assets requiring protection.	✓
6. Assign risk to asset/data owners.	✓
7. Understand the threats most likely to affect the organization.	✓
8. Understand the vulnerabilities that exist within the enterprise.	✓
9. Adopt an accepted risk management framework and/or standard.	✓
10. Create a standardized risk assessment form to evaluate risks to the organization.	✓
11. Create a risk register to track risk scores, risk treatment and residual risk.	✓
12. Perform risk compliance monitoring, including third parties.	✓
13. Communicate risk treatment and risk management to the organization.	✓
14. Continuously monitor the organization and assets for emerging risks.	✓

Table 2: Risk Essentials Program Checklist

According to the authors of "The Essentials of Risk Management" [11], risk management is a process of understanding cost and efficiently managing unexpected levels of variability in the organization. However, several existing frameworks have specific definitions or process flows. At the core of each, they all share the same underlying goals. Managing risks requires identifying, analyzing, and controlling risk exposure. The following figure summarizes the risk management process:

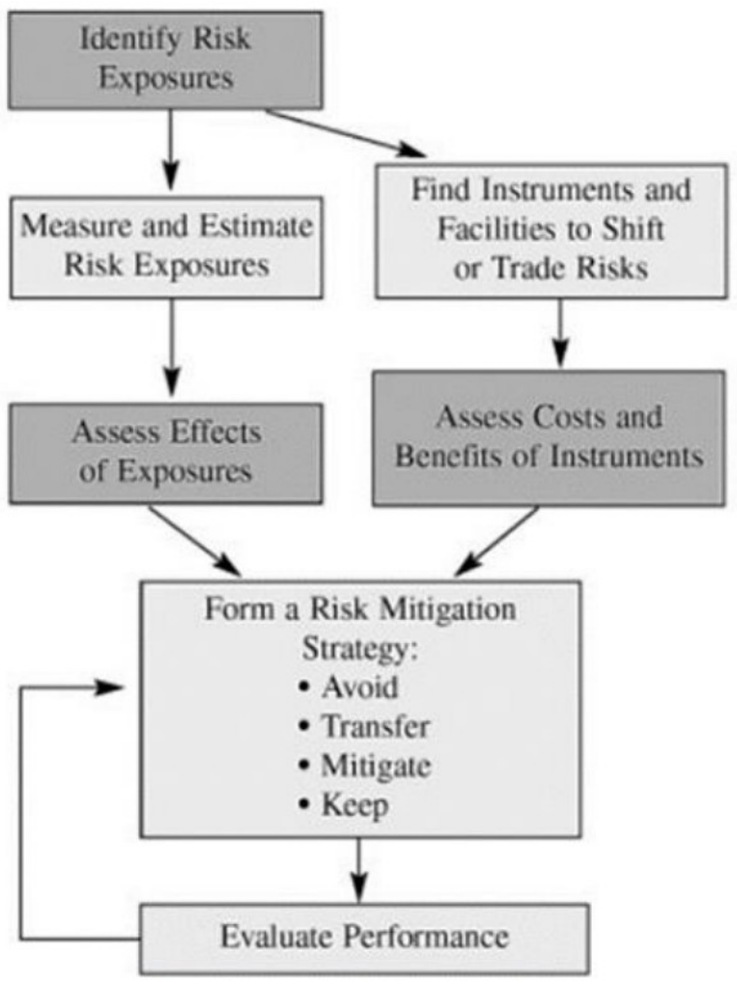


Figure 5: Risk Management. Source: "The Essentials of Risk Management"

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.3. Where Risk Resides

To help understand the application of risk management essentials, CISOs need to understand that risk does not just appear and know where it resides. Risk is a product of threat agents or vectors that can trigger an event. An event is triggered when a threat can exploit a weakness or vulnerability that exists within an asset. Risk can be raw or inherent, such as unboxing a new computer system. Every piece of computing hardware typically comes with vulnerabilities straight from the factory. For example, all logical and physical ports may be open, have default configuration settings implemented, etc., resulting in inherent risk. They are considered treated risks after closing the logical ports, changing environments, and applying controls such as physical port locks.

The figure below shows the confluence of threats, vulnerabilities, and assets that result in risk.

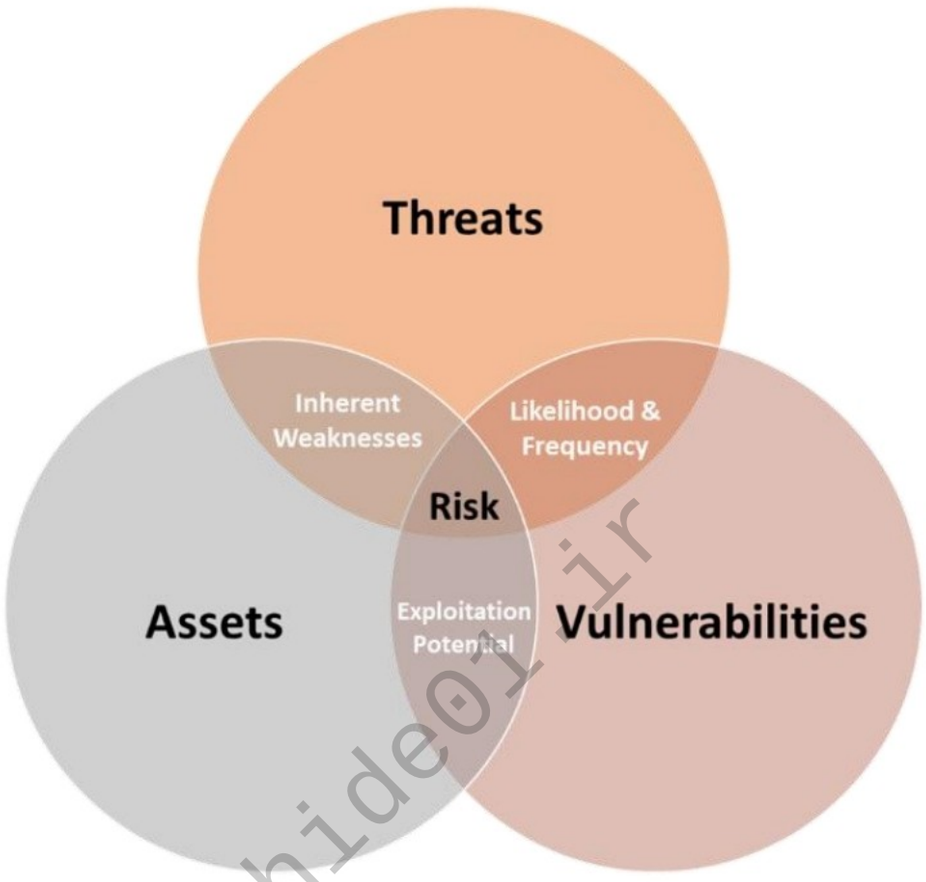


Figure 6: Risk Confluence Diagram

Risk managers, including CISOs, must learn how to balance threats, vulnerabilities, and assets to ensure investments in risk treatments do not exceed the value of the protected assets.

6.4. Risk Ownership

The complexity of determining risk often involves issues of internal organizational politics, everyday vocabulary, budgetary constraints, the concept of risk ownership, and the willingness of senior leadership—even the board of directors—to accept the responsibility for risk treatment. In addition, there is a need to execute the requirements imposed by the various stakeholders involved in the risk management process. The information security group does not own the risks within the broader organization. It has neither the authority nor responsibility for determining which risks will be treated and which will be accepted. The information security function is responsible for performing risk assessments, recommending risk treatments, and monitoring the execution of the risk treatment plans approved by risk owners and senior leadership. It is the CISO's job to lead the organization through understanding risk and then providing options for treatment.

CISOs do not typically perform risk assessments unless an organization is exceedingly small; instead, CISOs facilitate the process and function as a resource while a risk assessment team conducts the risk assessment. The information security team (or outsourced vendor) will complete organizational risk assessments, while project managers will be responsible for project risk

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

assessments (which can include information risk assessments). At times, it can be difficult to convince members of the organization responsible for projects to perform risk assessments.

What is most interesting about risk assessments is that we are all taught at an incredibly early age how to perform a risk assessment and create a risk treatment plan (albeit informally). If you ask the organization's employees if they know how to perform a risk assessment, they will say no. However, they could articulate how they avoided a risk while driving to work that day.

Understanding and mitigating risk is a skill that every parent, grandparent, or guardian imparts to children at an early age. We all know how to do it; it is ingrained into our psyche that we look both ways when we want to cross the street. This act of looking both ways is a risk assessment. We are attempting to determine the odds of safely crossing the street.

6.5. Risk Assessment Types

There are two basic ways to conduct a risk assessment. One is objective (quantitative), and the other is subjective (qualitative). Quantitative assessments focus on numerical values such as dollars, whereas qualitative assessments are more perceived value-oriented, providing results in general terms like high, medium, or low.

The following table shows the differences between objective and subjective risk assessments:

Category	Quantitative	Qualitative
Perspective	Objective	Subjective
Difficultly Level	Complex	Simplistic
Time to Complete	Long (Time consuming)	Short (Fast track)
Results	Numerical	Ranges or categories
Threat Frequency Calculation	Required	Optional
Automation	Risk assessment product recommended	Easily accomplished with spreadsheets
Pre-work	Requires substantial amount of research and data in advance	Limited, based mostly on opinion or what if scenarios
Asset	Requires understanding of asset values	Asset estimates are sufficient

hide01.ir

Table 3: Risk Assessment Types

6.6. Risk Assessment Process

ISO 27001:2017 sections 6.1.2 and 6.1.3 are used as a guide for risk assessments (a few liberties will be taken since we are not using an information asset in this example). First, we identify the risk. To illustrate risk, we can use an example from everyday life.

- Identify the asset(s). That would be you, the individual crossing the street. You are an asset.
- Identify the threats to the asset. Those would include the vehicles driving on the road—cars, trucks, motorcycles, bicycles—that might inadvertently attempt to occupy the same space you are trying to occupy simultaneously.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify the vulnerabilities that the threat might exploit. In this case, the vulnerabilities include the natural frailty of human life.
- Identify the impacts that the threat may have on the asset. This is obvious to adults but only so clear to a child once it is explained. If a car, truck, or motorcycle impacts the asset, at best, it will result in scrapes and bruises.

So, now we have completed the first step. We are the asset, the threats are the vehicles, we are vulnerable to those vehicles (at least until someone invents an individually portable force field), and of course, we understand the potential adverse result as the car, truck, or motorcycle and a human being collide. Next, we analyze and evaluate the risk.

We assess the impact that might result from the risk manifesting itself. In this case, it might be injury or worse. Therefore, our parents, grandparents, and guardians teach us to perform risk assessments—so that we can understand the risks and analyze them. This is what we do as we look both ways.

Given the controls already in place, we then assess the likelihood of the risk manifesting itself. If no cars are coming, the risk is exceptionally low. If you are crossing at a crosswalk, the cars are supposed to stop (at least in much of the world); if a school crossing guard is holding a sign (another control), then again, the likelihood is reduced. A crosswalk with a walk sign is lit, or there is an underpass or overpass (a further control) that might further reduce the likelihood of that vehicle colliding with you.

Given the conditions, we assess the level of risk of crossing that street.

And finally, we determine whether the risk is acceptable or requires additional controls. For example, you would walk up to the corner, press the signal button, and wait for the walk sign to be lit before crossing.

hide01.ir

The next step is to identify and evaluate options for treating risks.

As noted, we could apply appropriate controls—walk to the corner and cross with the light.

We could knowingly and objectively accept the risks—many kids would look both ways and, knowing they are invincible and immortal, will scamper across while Mom looks on in horror. We will talk about this in a moment. We could avoid the risk entirely and abandon our journey.

Another option is to transfer the risk to another party. We do this already to some extent in the form of medical insurance, although in this case, most individuals would not consider this one of the best options to treat the risk, and indeed, most parents would agree there are better options.

The next step in the ISO 27001 standard is to select control objectives and controls to treat risk and then obtain management approval of the proposed residual risk. In the scenario of a child crossing the street, the parent, grandparent, or guardian's attempt to mitigate the risk starts with teaching the child how to perform a risk assessment and suggesting control objectives and controls to avoid harm. Hopefully, the child has learned the lesson, but most parents, grandparents, or guardians will evaluate their children and verify that the lesson is learned. This is an opportunity to provide feedback and approve the child's choice. The child scampering across the street while the mom looks on in horror is where this last step of obtaining management approval is essential. The parents, of course, would approve of walking to the crosswalk but would not approve of the child running across the street without looking first.

When discussing the performance of risk assessments with those who have never conducted one

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(or at least they believe they have never done so), it is crucial to make the topic relatable. If they were to be handed a copy of ISO 27001 or 27005 or even a risk management manual, they would certainly not read, understand, or care about it. Use the street crossing example or make up your own, but the key is getting employees and the organization to understand risk assessments and the risks they might encounter as they do their work.

After the risk assessment has been performed, the treatment plan is used to provide an understanding of the types of controls that can be implemented and the objectives of those controls. Security controls exist to mitigate risks to the organization, and a wide variety of them exist. First, there are automated controls and manual controls. Each has its place, and each can provide value in mitigating risks. Next are technical and management controls, such as policies and procedures. Organizational norms and culture can also influence the effectiveness of control objectives that organizations choose to pursue.

CISOs are frequently forced to focus more on technical controls than designing policies, standards, and procedures. However, it is important to also focus on understanding organizational culture and implementing management controls. A CISO's job is to work within both a business and a technical framework that requires understanding the company, its company culture, and its goals. The role of the CISO is to guide decisions and recommend effective controls that senior management will approve and fund.

Part of choosing controls to mitigate risk is creating a governance program that can assist in implementing a framework that provides an appropriate level of assurance that security risks are professionally managed. A CISO's mission is to lead the information security team in evaluating, measuring, and monitoring controls to determine their effectiveness. The goal should be to identify performance metrics that help identify whether the program is effective and efficient for managing organizational risk. To measure and monitor control effectiveness, the CISO will also continually evaluate whether automation can be implemented to reduce or repurpose human resources to continually improve risk management. CISOs rarely have enough well-trained security personnel on staff. By implementing good processes and reviews, learning how to use available resources most efficiently should be possible. CISOs should consider ways to improve controls to measure and monitor control effectiveness.

In Domain 2, there will be a focus on managing the audit process. This audit process will validate the controls that are chosen to be applied to manage the risks that have been identified. In other words, risks are assessed, and risk treatment plans are created. Assessments or audits are performed to evaluate whether those risks have been appropriately mitigated. The interconnectedness of the domains in this body of knowledge is key to the foundational success of understanding and treating risks.

6.7. Risk Categories

The two primary categories of risk are as follows:

- **Inherent Risk**

  Inherent risk defines the risk that exists before controls are implemented. The organization must understand the potential risk impact before controls are implemented to realize the value and effectiveness of the mitigation strategy.

- **Residual Risk**

  The most important concept of risk management is that some risk remains after controls

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

are applied. Risk mitigation exists to reduce risk to an acceptable level, but that level is rarely zero unless the organization chooses avoidance as the risk treatment strategy. Risk acceptance, therefore, is an expected outcome of reducing risk to the lowest acceptable level.

Figure 7: Residual Risk Formula

Once the risk treatment options are chosen, validating the residual risk to the organization is crucial. The risk assessment team (and the CISO) will need to clearly articulate recommended risk treatment and the expected residual risk that will be retained/accepted by the organization. The complete recommendation by the risk assessment team is made only after the entire proposal, including treatment recommendation and analysis/documentation of residual risk, is provided to the business leadership to make risk decisions.

When communicating residual risk, it is essential to place it into the context of the risk acceptance criteria by clearly indicating how the business impact and/or likelihood has changed based on the recommended risk treatment and then how the resulting combination of effect and probability is reduced to meet risk acceptance criteria as previously discussed. Preparing for questions from the business team and making final organizational risk decisions will be advantageous.

Decision makers will likely want to know what additional controls there might be to further treat the residual risk and the approximate cost and risk mitigation benefit of additional risk treatment. Further treatment and/or additional controls to lower residual risk typically increase the controls cost. The CISO and risk assessment team will be prepared for the discussion by thinking through likely follow-up questions. This will also help the CISO gain credibility as a well-intentioned business partner interested in cost-effective solutions to business problems and not just someone interested in building a security empire.

6.8. Risk Treatment

Risk treatment is a process for modifying risk. Risk treatment can include:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.
- Accepting or increasing risk to pursue an opportunity.
- Removing the risk source.

You can also modify the risk by changing the likelihood and the consequences, sharing the risk with another party or parties (including contracts and risk financing), or simply retaining the risk as an informed choice.

Risk treatment is a business decision. The CISO supports the decision-making process by identifying risks and recommending treatment options. The business owner must choose the

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

treatment option for the risk most effectively supporting the organization's goals. The CISO may offer options related to risk treatment, but the final decision belongs to the business.

The ultimate reason for a risk assessment is to perform effective risk treatment that helps the organization meet organizational goals. This is where the specialized skills of a CISO with a broad understanding of the business, business processes, technology, and people are essential in advising the senior executive(s) responsible for approving the risk treatment plan. Being able to function as an effective facilitator between the team performing the risk assessment and the business leadership empowered to make the business decisions that result in a balance between risk and reward can heavily influence the success of a business. Conversely, being ineffective can contribute to the company being ineffective, or in a worst-case scenario, a company-ending event.

The CISO's role is advisory to help business leaders agree to risk recommendations. Or, if agreement is not possible, the goal is to ensure they understand the implications of choosing an alternate risk treatment plan. When business leadership decides on an alternate risk treatment, the CISO's position shifts from being an advisor to one who advocates for the recommended risk treatment. This is a subtle but significant shift. This sometimes requires political prowess, but it is important to remain firm if the alternate risk treatment is inappropriate for the organization. The business leaders involved in this process will make choices that reduce the costs of risk treatment. The CISO's job is to register a firm disagreement unless swayed by their rationale. Understand that nobody else at the company will advocate for more strict controls than the CISO— there is typically no one else who will argue against the loosest of controls or risk acceptance.

However, the risk treatment decision is not the CISO's to make. This is a business decision, and the CISO is typically not the decision maker. This makes sense as the CISO occupies a support role within an organization, and few CISOs have operational revenue-generating responsibilities.

Once the business leaders have listened to potential solutions, completed their evaluations, and chosen a risk treatment, the CISO's job is complete (unless responsible for implementing/managing the control selected).

How do risk treatments work exactly?

First, take the output from the risk evaluation step, which is the list of prioritized risks. Then, select each one in priority of criticality, review the process used to perform the risk assessment, and do a review to verify that the risk assessment results were accurate. The last step is to put together the recommended risk treatment plan.

ISO 27005 includes a diagram that concisely illustrates the process discussed in this section. This diagram provides the process of risk assessment to risk acceptance.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

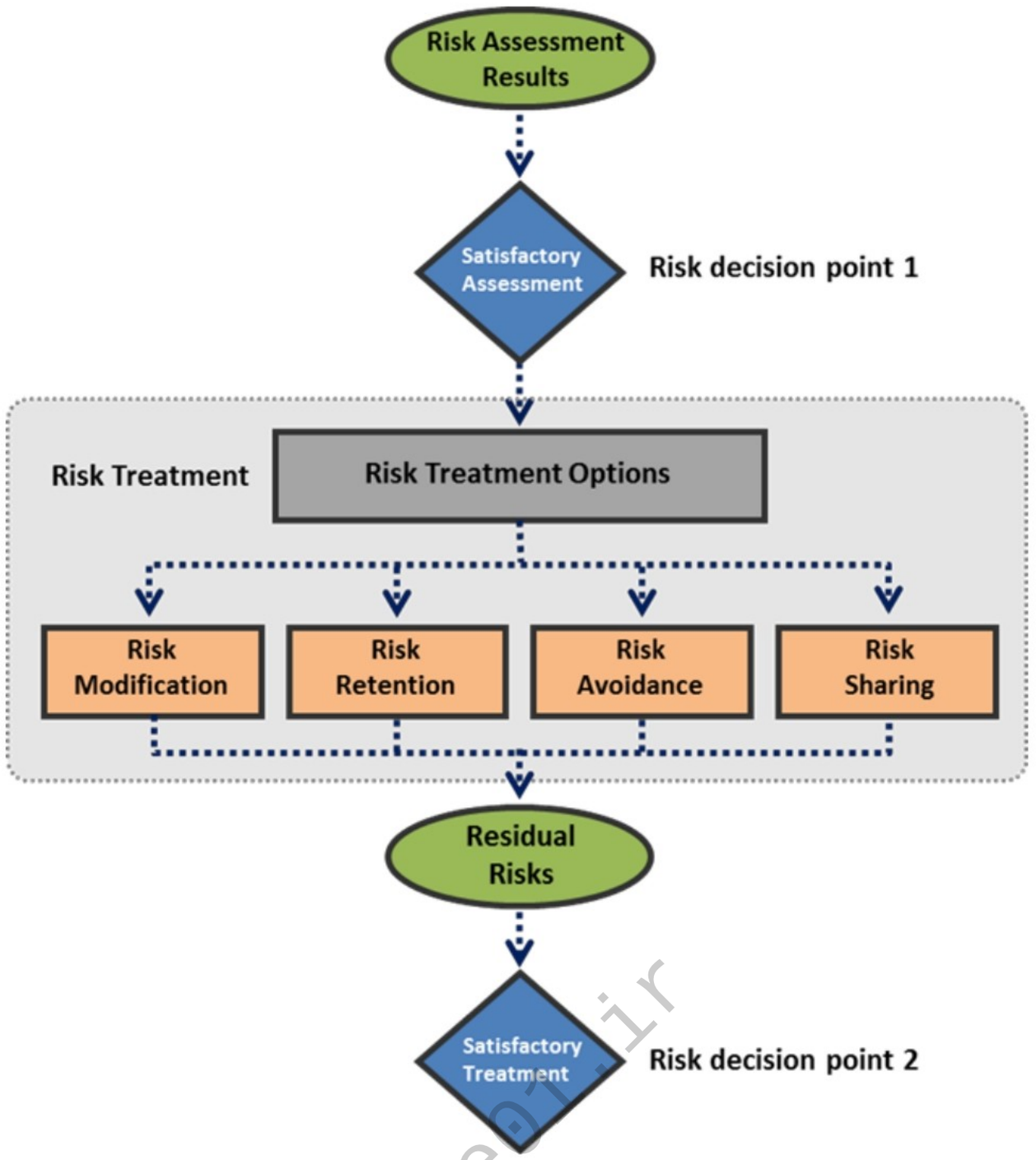


Figure 8: ISO 27005 Risk Treatment Activity

Defining some inconsistent terms between ISO 27005 and ISO 27001 is important. Within ISO 27005, "risk retention" is used instead of "risk acceptance." Risk acceptance is the more commonly understood term used in ISO 27001.

The more common term for "risk modification" is "risk reduction." Sometimes, it is appropriate to either remove an expensive or ineffective control and accept the risk (risk retention) or alter the control by replacing it with a more effective (or cost-effective) control that still meets the criteria for accepting the residual risk. Hence, the term "risk modification" more accurately reflects potential risk treatment since the risk treatment may not always be a reduction of risk.

Finally, "risk sharing" is often stated as transferring risk. This term is less commonly used because of how easily it can be misunderstood. There is no way to transfer risk entirely to another organization. The risk is still inherently owned by the organization; however, some of the impact, if realized, can be shared. One example is when an organization engages an outsource partner to provide a service. Should the outsource partner be breached, the organization has a higher probability of being breached. Clients and customers will blame the primary organization and not the third-party vendor for the breach since they hold that organization responsible for the security of their data.

Having a vendor breach impact your organization could also be considered a need for due diligence in choosing the breached vendor. The organization will still be held accountable and will still be damaged. In this scenario, the risk was not fully transferred.

Let us proceed with the topic of risk treatment. We will continue using ISO 27005 as the basis for

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the discussion. The organization's specific risk framework may differ in detail but not in treatment methods.

There are four options when it comes to risk treatment:

- Modification
- Retention
- Avoidance
- Sharing

6.9. Risk Modification

Risk modification is the most typical approach for managing a risk. This method usually results in recommended controls for managing risk. ISO 27005 guidance for this section is that "The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be re-assessed as acceptable."

This is part of the risk assessment/risk management process, where the experience of the CISO is coupled with an understanding of the business goals and strategy. The focus of the CISO and security team is to propose controls that help the organization meet its risk goals while simultaneously limiting cost and disruption to the business when implementing them.

At this point, the CISO must balance many different business interests apart from being cost-conscious. Legal and audit will be concerned with compliance, sales/manufacturing/operations will want to be assured that business is not impeded, and other senior staff will want to ensure they can still deliver on their commitments despite recommended security controls. Balancing these interests is extraordinarily important and needs to be done as each broadly impacts management. The reputation and trust in the CISO and the information security team can easily be damaged should this process of considering each stakeholder's interests not be analyzed and included in the recommendation process.

As part of this process, there could be a temptation to play different organizations against each other. If the organization's internal politics are such that this technique would be helpful, pursuing that course of action might be necessary. However, it is usually a risky approach. It is better to retain the appearance of being above those types of actions, acting as an honest broker. Machiavellian political intrigue is usually not used to pursue the organization's best interests.

The CISO needs to ensure that selected controls provide the following types of protection (according to ISO 27005) — "correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring, and awareness." When choosing controls, consideration for all costs (acquisition, implementation, ongoing administration, operations, and monitoring) must be clearly understood. Costs must always balance with the risk mitigation capability of the chosen control and align to the asset's value being further protected.

It can be challenging to do this correctly all the time. The goal is to do the best job possible, function as an honest broker, be prepared for the discussion with senior management, and have alternatives ready for discussion. These alternatives may be less expensive or difficult to implement but may also be less effective than the primary recommendation. In conversations regarding recommended controls, there will be a need to justify the control selection and cost concerning the level of risk and risk mitigation approach. It is a virtual certainty that return on investment will be discussed. Compared to the cost of implementing the control, the cost of an untreated risk is

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

significant to understand and clearly communicate. If the return on investment is negative, likely, the control will not be implemented. If this is the result, it is important to consider alternatives or ways to minimize costs for the selected control to realize a positive return on investment.

To do a Return on Investment (ROI) calculation, it will be necessary to do some math and produce a cost should the risk manifest itself. The most common way of doing this is to estimate an Annualized Loss Expectancy. This simple calculation is beneficial. Understand that the longer the business has operated with the risk, the more difficult it will be to convince business owners to apply mitigation and controls. Senior management will typically push back on the likelihood portion of the calculation.

The ALE is a standard ROI-supporting calculation that applies to selecting controls.

Annualized Loss Expectancy (ALE) = the cost of the risk manifesting × the likelihood of the risk manifesting in a single year.

For example, if a risk manifesting would cause $1 million in damages and clean-up costs, and the likelihood of the threat manifesting within a given year is 5%, then the ALE would be $50,000.

Let's assume the cost of the control to manage this risk is $25,000/year and the likelihood is thus reduced to 1%, then the Annualized Loss Expectancy would be reduced to $10,000/year at $25,000/year control cost with a potential savings of $15,000/year (original Annualized Loss Expectancy of $50,000 minus the cost of controls $25,000 minus the reduced Annualized Loss Expectancy of $10,000 results in a $15,000 savings or ROI). In other words, you paid $25,000 for a control to reduce your ALE by $40,000 resulting in a $15,000 savings or ROI.

Going back to the discussion of control alternatives—the alternatives should include controls that are both more and less expensive. The CISO should scrutinize control costs to reinforce with senior management that alternate controls that could provide additional mitigation have been considered but discarded as not cost-effective or otherwise unnecessary. This will bolster the department's credibility during the discussion as the CISO will be perceived as not just advocating for the strictest controls but instead trying to balance the risk with integration with the interests and goals of the business.

It is critical to clearly explain why the alternate risk treatments are less optimal than the recommended risk modification. If guiding a risk modification, be ready to explain the other possible risk treatments and how they are inappropriate for use within the circumstances. Also, make sure you point out that the residual risk (whatever risk remains after the control is applied) will be treated following one of the other risk treatments (often risk retention or acceptance; however, risk sharing, such as insurance, can also occur).

Choosing specific controls occasionally goes beyond balancing the cost and risk mitigation provided. Other inputs into this process are necessary. The first one is compliance or contractual requirements. There are reasons for choosing controls because they must comply with regulations/laws in a particular domain. For instance, if the analysis were to be done using Annualized Loss Expectancy and the required control costs more than the Annualized Loss Expectancy, then it would be likely that the control would be implemented with a compliance requirement. A compliance requirement would be an excellent reason to implement a control regardless of what the risk assessment might suggest.

The second reason a control that is not otherwise cost-effective might be implemented is that everyone else does it. Therefore, there is an expectation that control is in place. This could be the case when it comes to antivirus software. Arguments can be made that commercial antivirus

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

software is not cost-effective; however, there is an expectation that this control should be in place because everyone has this control. This should not be considered a good reason to do something; however, the reality is that this or something similar could be confirmed within the environment.

ISO 27005 conveniently points out some significant constraints to consider as part of this process:

- **Time constraints**: Sometimes, the proper control will take too long to implement. It might be better to install a solution that reduces risk now rather than wait much longer for the best control to be implemented.
- **Financial constraints**: The CISO needs to understand the costs and benefits to the organization and must function as a good steward for the organization's finances when controlling implementation and maintenance. Controls that cost more annually than the calculated Annualized Loss Expectancy are candidates for removal or modification. The exception to this is when control is a mandatory compliance requirement or contractual obligation.
- **Technical constraints**: For example, an inability to find controls that will not reduce or render a system nonfunctional or so impaired that the solution and implemented controls are useless.
- **Operational constraints**: If a control takes so long to implement and perform properly that it delays the functional use of systems beyond the change control window, this can result in business issues. Another example is if a requirement exists to deliver a solution during a brief period and results in a breach of contract and loss of goodwill, the cost could be more than the risk the control was designed to mitigate.
- **Cultural constraints**: It is important to remain sensitive to cultural norms when considering controls, particularly those used internationally and involving people. If a control is rejected because of a misunderstanding or impact on cultural norms, it could be solved through additional training to help those resistant to the control understand why it is being applied. If the situation cannot be resolved, alternative controls might be necessary.
- **Ethical constraints**: Ethical constraints can be like cultural constraints. Ethical considerations are cultural, although there are differences. One example in the ISO 27005 documentation involves privacy.
    - In some societies, privacy considerations are more strictly enforced through legislation. In other societies, privacy considerations are much less critical. Implementing SSL packet inspection of encrypted data in one country or region might be completely acceptable. At the same time, it could cause issues with employees or customers, as they might consider such behavior by the company to be unethical.
- **Environmental constraints**: The perfect example of this is the probability of significant environmental events based on location. Some locations have a propensity for tornadoes, some experience an elevated level of flooding, while others have earthquakes. Earthquake preparation is necessary in some areas of the world, whereas buildings are reinforced to withstand ground shaking. In others, below-ground reinforced structures to withstand a hurricane or tornado might be required. A CISO must clearly understand the environment where controls are being considered.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Legal constraints**: The CISO fortunately has someone to lean on for help with this constraint, namely the organization's legal counsel. As mentioned earlier, compliance with regulations and other legal issues is critically important. Laws and regulations must be managed accurately, and for some industries, compliance will be a critical consideration (such as healthcare, financial services, government, energy, etc.).
- **Ease of use**: When considering controls, consider how people use the organization's systems and services. Then, think about how their use of the systems might be impaired if specific controls were implemented. The argument about multi-factor authentication has historically been a critical control that involves user experience. Do spam filters make users feel that they lost e-mail and thus require frequent checking of spam folders? Ease of use should always be considered. If a security function does not carefully consider it, user complaints can be expected.
- **Personnel constraints**: The CISO needs to know what is possible with available personnel resources and plan accordingly. If additional personnel are required, or personnel need to be trained to operate controls effectively, other resources should be considered. With good planning, a CISO can minimize this risk by hiring experienced operators or providing training to existing staff.

New controls need to integrate well into the broader set of existing controls. An alternate control should be considered if the control does not work well with existing controls. Suppose the new control requires that an existing control be changed or reconfigured. That should be evaluated to determine if the new control is cost-effective or sufficient for mitigating risk.

6.10. Risk Treatment Options

Organizations have four options to support their risk treatment strategy. The term used to describe the strategy depends on the risk management framework selected by the organization. All frameworks use a familiar concept, but the language or terms might vary. For example, NIST and ISO use different terms in their discussion of risk treatment, but the terms are synonymous and produce similar outcomes.

The following is a graphical depiction of risk treatment options:

Figure 9: Risk Treatment Options

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.10.1. Risk Modification or Mitigation

Risk modification is the most common risk treatment option. When applying modification, an organization seeks to change risk exposures or outcomes by implementing security controls to a process, system, or environment. Some risk management frameworks describe modification in terms of mitigation—the extent to which the severity of the risk has been reduced. Because modification is commonly associated with the application of security controls, the CISO must understand the types of controls available and the objectives of those controls.

What is control?

A control is a measure that modifies a risk. Controls for information security include any process, policy, *procedure, guideline, practice, or organizational structure and can be* administrative, *technical, managerial, or legal that modifies information security risks. Controls may not always exert the intended or assumed modifying effect and must be audited to assure effectiveness. A control can also be called a safeguard, countermeasure, key control, or compensating control.*

6.10.2. Risk Retention or Risk Acceptance

Risk acceptance often occurs when an organization acknowledges the existence of a risk and deliberately chooses to operate without further modification or the application of a treatment option. The organization accepts the potential outcome of the identified risk while understanding the potential impact on the organization. Some level of risk always exists, even after applying controls to support mitigation. Risk acceptance in this manner applies to the remaining or residual risk.

Risk acceptance often maps to the organization's perceptions or feelings about risk. The CISO is responsible for communicating the risk and potential outcomes, but the organization is responsible for choosing whether to accept risk as a treatment strategy. This is typically done by business owners responsible for primary operations or revenue generation within the organization. The CISO should define policies and procedures for risk acceptance as part of corporate governance. Optimally, the policies and procedures should specify requirements for escalation and approval of risk acceptance to provide accountability for these decisions.

Whether or not a risk is treated, risk retention or risk acceptance is always within the risk management program. The variable in the process is whether there will be some level of risk treatment in addition to risk retention. The evaluation and resulting decision depend on the cost to the business in terms of time, people, and finances.

As mentioned earlier, residual risk remains after one of the various treatments is applied. This risk is either further treated, retained or accepted. There is no harm in making a business decision to maintain a risk. However, the CISO is responsible for clearly communicating risk status within the organization to senior management. It is never possible to eliminate all risks. Even if it were possible to get close to doing so, the cost to the organization would be enormous. It is essential to communicate this concept in extremely risk-averse environments. The CISO provides the methods and processes for measuring and communicating residual risk to senior leadership to support accurate decisions to retain or accept the risk.

If senior management is unwilling to accept the residual risk, additional options must be explored. Senior management must either retain or accept the risk or release funding to treat the risk further, using other controls to modify, avoid, or share the risk. If senior management

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

continues to be unwilling to decide risk disposition, retaining or accepting risk will be the default course of action. This typically happens because of ignoring the risk due to the lack of financial budget. The CISO normally can only spend money on risk treatment with senior management approval. This scenario results in risk retention and will generally require communication with senior management personnel, informing them of their decision by not funding any other course of action. By not deciding, a decision was still effectively made.

6.10.3. Risk Avoidance or Risk Elimination

Avoidance is a risk treatment option when an organization changes or avoids an activity by removing the risk and eliminating its effect on the organization. For example, an organization may choose to build a new facility because of the outcome of a risk assessment. Instead of applying controls to address natural disasters or other physical threats within a current location, the organization builds another site to eliminate the identified risk.

When an action by the organization would be too costly or difficult to implement, choosing not to pursue that action or activity is the typical result. ISO 27005 mentions that "for risks caused by nature, it may be the most cost-effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control."

Situations that fall into this category are usually discovered post-implementation. Things like locating a nuclear power plant near an earthquake fault line or along a coastline that is susceptible to frequent tsunamis naturally seem risky in hindsight. Another less obvious example could be offering a line of service as a PCI-DSS Qualified Security Assessor for companies that perform large numbers of credit card transactions, creating the potential for unlimited liability from within a targeted customer base.

6.10.4. Risk Sharing or Risk Transfer

Risk sharing relates to reassigning accountability for a risk to another entity or organization. Most often, this is accomplished by purchasing insurance that will reduce the direct costs of a covered event or remediation. This risk treatment option also applies to the distribution of risk between business partners. Although shared or transferred risk can reduce costs associated with risk management, an organization cannot transfer risk entirely to another organization. The organization owns the risk and communicates the impact of potential outcomes.

Risk transfer is an acceptable strategy to manage easily defined or clearly understood risks. Risks that are difficult to quantify may increase the risk profile because a loss of influence or control is assumed when an organization transfers or shares risk with another entity. For example, cyber insurance may provide coverage for a data breach, but the policy might only pay if specific criteria associated with a breach are met. Root causes and outcomes can vary widely from one organization to the next.

Risk transfer will allow an organization to better manage risk and often times do it more cost-effectively. As mentioned, cyber insurance is the primary method used to transfer or share risk. Suppose the risk manifests, and operational capabilities, business functions, or revenue are lost. In that case, insurance payments will either reduce the direct costs of the incident or completely take care of the costs of the incident and clean-up. Note that this approach does not solve issues related to losing customer confidence or losing partner relationships.

Another example of risk sharing would be when the organization outsources management of a specific function (such as the Security Operations Center) or security solution to provide

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

faster response or more effective results than if the organization managed the operation.

In either case, purchasing insurance or outsourcing an activity to mitigate the risk creates a cost to the organization. Purchasing insurance or outsourcing functionality needs to be evaluated with the cost of direct risk treatment. When transferring risk, there is typically an additional cost that the organization cannot share. This is the cost of the blame for the risk manifesting itself. The organization will be responsible and could end up with brand damage and loss of goodwill regardless of cost recovery via insurance payout.

Additional risk is present when outsourcing business activities. When a third party participates in treating risks, this, in turn, can introduce other risks. What if the outsource partner is compromised and becomes the vector of attack that disrupts you, the customer? CISOs typically require that risk assessments be performed on vendors to support critical business or security functions within the organization. This provides proof of due diligence. The additional cost of conducting risk assessments on critical vendors needs to be factored in as part of the cost of risk sharing when comparing alternate risk treatments.

6.11. Applying Compensating Controls to Reduce Risk

Once risk has been identified and quantified with a risk score, the next important activity is to determine disposition. If the choice is made to reduce it by offsetting the risk condition, the CISO typically recommends safeguards or controls that could be derived from an existing regulation or standard. When an organization cannot apply the recommended risk treatment, compensating controls can be considered an alternative approach for reducing the risk.

Compensating controls can be applied when an organization cannot use the recommended controls due to business or technical constraints. Compensating controls should satisfy the following criteria:

- Meet the intent and rigor of the original requirement.
- Provide a similar level of defense as the actual requirement.
- Exceed original recommended or stated requirements.

Compensating controls are more accessible but often times more expensive or less adequate to deploy and should be used as a last resort. Most organizations view compensating controls as temporary until full control compliance can be achieved.

The following is an example of compensating controls that could be applied when an organization is not able to deploy a recommended standard control for segregation of duties due to limited staff:

- Increase audit logging and monitoring of transactions.
- Invoke multiple layers of supervisory oversight of critical transactions.
- Require full exception reporting on nonstandard transactions.
- Increase physical auditing of duties and activities.

6.12. Risk Calculation Formula

If we were to build a gathering place for a specific holiday, the busiest day would be when the entire gathering of people attends. The construction cost would not be beneficial for the use of the facility. Instead, we want to know the average number of attendees each day and spend

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

resources on the average to build it to a reasonable specification. If we consistently exceed capacity, we can add extra facilities.

Estimating the number of times, a threat occurs requires the same type of thinking; only we have a formula called Annualized Loss Expectancy (ALE) to help us. The ALE is the estimated monetary loss that can be expected for an asset annually. In risk management, we typically use ten years. ALE includes the following components:

- **Asset Value (AV):** The value you have determined an asset to be worth. Assets can be information, cyber assets, or even intangible concepts such as the value of reputation or goodwill. A tangible value might be a customer data record value of $7 each; if you had one million records, the collective asset value would be $7 million.
- **Exposure Factor (EF):** This is the estimated percentage of damage or impact a realized threat would have on the asset. The range is zero to 100%. The concept is that exploited threats do not result in 100% loss during a cyberattack, but a loss of valuation or cost is associated with an event.
- **Single Loss Expectancy (SLE):** This is the asset value multiplied by the exposure factor and determines the expected loss for a single event. If we were to estimate that we expected only 25% of our records to be compromised, the SLE would be $1.75 million of our $7 million asset value.
- **Annual Rate of Occurrence (ARO):** The last number we need to determine for our formula is how many times we expect the threat event to occur over a year. We would use our organization's experience or research-reported averages to achieve this. ARO ranges from 0.0 (never) to 1.0 (always). If you were to select 1.0, you would state that the event happens once every year. If you specify an ARO of 0.1, you say it will happen 0.1 times over one year.
- **Annualized Loss Expectancy (ALE):** Arriving at our final calculation, we take the SLE multiplied by the ARO to determine our estimated annual loss. The ALE spreads out the expected loss over a year. The table below presents the formula for deciding ALE.

ALE Calculator				
Asset Value (AV)	**Exposure Factor (EF)**	**Single Loss Expectancy (SLE)**	**Annual Rate of Occurrence (ARO)**	**Annualized Loss Expectancy (ALE)**
$7,000,000	**.25**	**$1,750,000**	**0.1**	**$175,000**
(AV x EF = SLE) x (ARO) = ALE				

Table 4: Annualized Loss Expectancy Model

6.13. Risk Management Frameworks

Numerous frameworks guide identifying, treating, and monitoring information security risks in an organization. Risk management frameworks provide the structure upon which an organization builds an effective risk management program. Risk frameworks are indispensable tools that can assist security managers in developing and implementing a robust security program and ensuring its continued success via monitoring. They include significant detail and provide specific

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

recommendations for managing and reporting risk. Frameworks are operational and provide detailed descriptions of how to implement, create, or manage a risk program or process. Risk managers need to understand how to use frameworks and direct the risk management program according to the guidance provided by a selected framework. Frameworks can be organized into four categories:

- **Cybersecurity Risk Management Frameworks** – A framework that is specifically targeted toward identifying, assessing, and treating risk within an information technology enterprise.
- **Enterprise Risk Management (ERM) Frameworks** – A framework designed to evaluate risk holistically throughout an organization. These are typically used by organizations to integrate internal controls, broader assets or holdings, supply chains, or other risk vectors to include technological risks.
- **Risk Assessment Methodologies** – These typically focus on assessing risk within assets and assigning a score. They provide specific tools and formulas to conduct a risk assessment.
- **General Risk Management Frameworks** – A generic framework applicable to any asset or scenario. These can be used in any business or industry. For instance, they could be used to assess financial, operational, or technical risk.

The following table presents the designation of the various risk management frameworks:

Cybersecurity Risk Management Frameworks	Enterprise Risk Management (ERM) Frameworks	Risk Assessment Methodologies	General Risk Management Frameworks
COBIT 5 for Risk (ISACA)	COSO Enterprise Risk Management Framework	Information Risk Assessment Methodology 2 (IRAM2)	IRGC Risk Governance Framework
Factor Analysis of Information Risk (FAIR)	RMA Enterprise Risk Management (ERM)	Facilitated Risk Analysis Process (FRAP)	Operational Risk Management Framework (RMA)
ISO/IEC 27005:2018 Information Security Risk Management	ISO/IEC 31000:2018 Framework and Process for Managing Risk		
NIST SP 800-37 Rev. 2 Risk Management Framework			
TARA (Threat Assessment Risk Analysis) Management Framework			
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)			
The Risk IT Framework - ISACA			

Table 5: Risk Management Frameworks

The CISO should select the risk management framework that best supports the organization. Some frameworks may be more effective in meeting the needs of the organization than other frameworks. For example, the risk management frameworks from ISO and NIST are comprehensive but require moderate maturity and significant resources to achieve the goals outlined within each framework. Other frameworks have narrower and specific objectives and are more tailored to meet the needs of smaller or less mature organizations. However, these may fail

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to provide a comprehensive program that larger and more complex organizations require.

The two most important risk management frameworks in use are ISO 27005 and NIST SP 800-37.

6.13.1. ISO/IEC 27005:2022

ISO 27005 provides information guidelines designed to give broadly acceptable guidance for information security risk management. The standard applies globally, supports wide adoption across industries, and maps directly to the strategy and recommendations outlined in ISO 27001 [12]. The ISO 27005 risk management process directs a structured sequence of steps to manage information security risks for processes and systems.

ISO 27005 Risk Management Process

- Context establishment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Communication and consultation
- Monitoring and review

All content in this section, in summary, and about the ISO Standard, is derived from the ISO 27005 guidelines. The catalog for ISO 27005 is cited as the reference because only informative sections of the standard are available for review without purchasing access.

hidel.ir

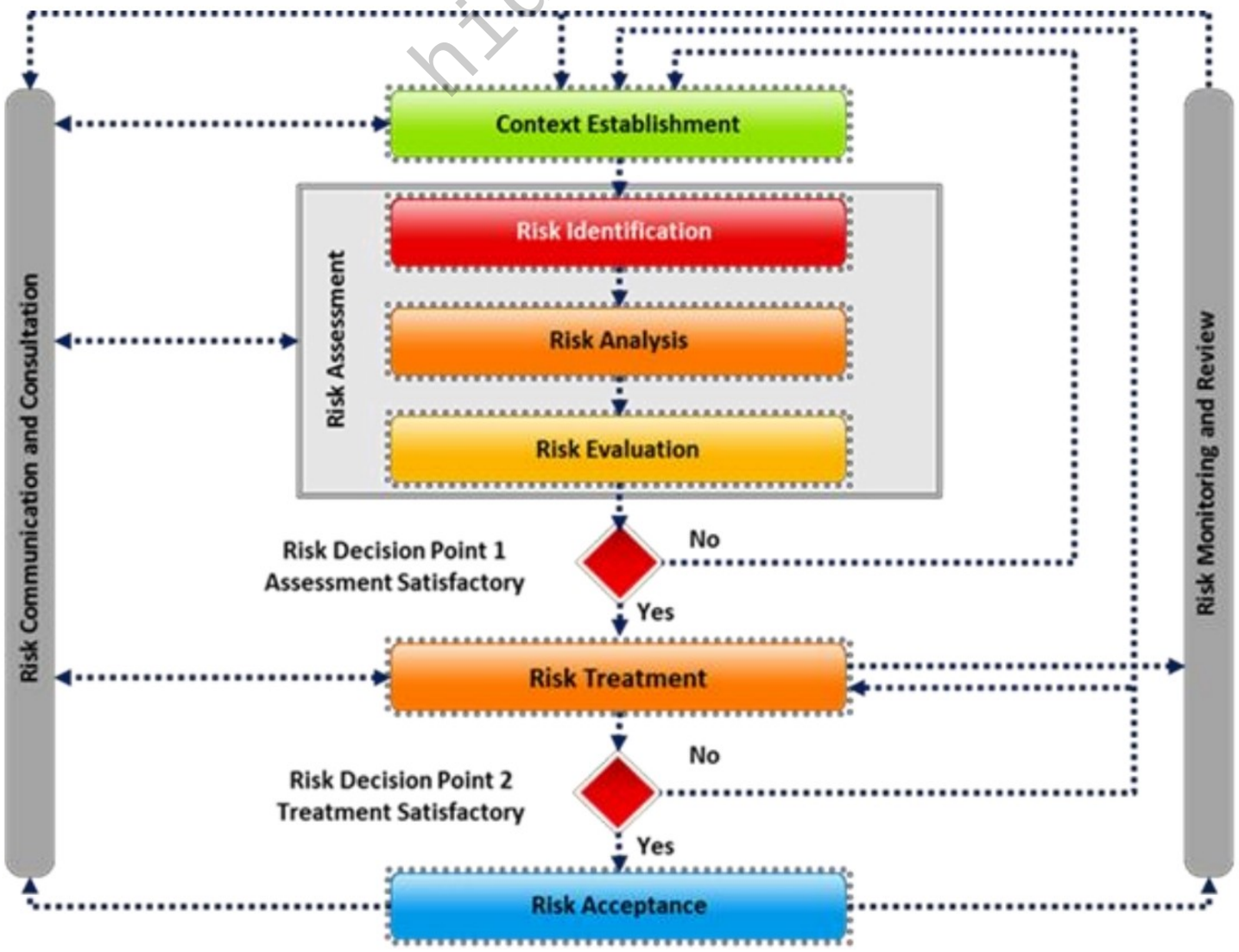


Figure 10: ISO 27005 Risk management process (Source: ISO/IEC 27005: 2018, "International Standard Information Technology-Information technology Security techniques -Information security risk management" (3rd ed.), Geneva: ISO Copyright Office. P. (4).)

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Each of the components of the ISO 27005 framework includes the following concepts.

6.13.2. Context Establishment

Clause 6 of ISO 27005 requirements establishes the context for information security risk management. Relevant inputs are gathered and evaluated when completing the process of context establishment. Business goals are a significant input. Existing policies, standards, and compliance also help build the context. Decisions such as risk evaluation criteria, impact criteria, and risk acceptance criteria are also defined and will be used later in the risk management process.

The context establishment process produces the outputs that support the risk assessment process. This output includes the essential criteria used to support a risk assessment, including the scope and boundaries of the risk assessment and the identification of the organization responsible for risk decisions. The responsibility for identifying and communicating information security risks within the context of ISO 27005 rests with the CISO. The CISO is responsible for the processes and methodology to complete risk assessments and maintain a record of the process and results.

- **Input**: All information about the organization relevant to the information security risk program's context.
- **Action**: Establishing the external and internal context for information security risk management involving organizational considerations (clause 6.1), identifying basic requirements of interested parties (6.2), applying risk assessment (6.3), establishing, and maintaining information security risk criteria (6.4), and choosing an appropriate method (6.5).
- **Implementation guidance**: It is essential to determine the purpose of information security risk management, as this affects the overall process and the context establishment. This purpose may include some of the following examples:
    - Supporting an information security management system (ISMS)
    - 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
- **Output**: Providing the expected information security risk management results

6.13.3. Risk Assessment

Asset value, threats and vulnerabilities, existing controls, and potential consequences are considered during the risk assessment step within the ISO 27005 risk management workflow. This information helps the organization create a prioritized list of risks that can be ranked according to the risk evaluation criteria specified in the context establishment phase.

Because the workflow is a cycle, risk assessments occur iteratively. The first iteration includes a high-level assessment to identify readily discernable risks that warrant further assessment. Additional iterations help refine the discoveries made in the initial assessment.

hideoi.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Input:** This involves the basic criteria, the scope and boundaries, and the organization for the information security risk management process being established.
- **Action:** Risks should be identified, quantified (or qualitatively described), and prioritized against the risk evaluation criteria and objectives relevant to the organization.
- **Implementation guidance:** A risk is a combination of the consequences that would follow from an unwanted event and the likelihood of an adverse event. A risk assessment quantitatively or qualitatively describes the risk and enables managers to prioritize risks according to the seriousness of the risk or other established criteria.
- **Risk assessments consist of the following activities:**
  - Risk identification (Section 8.2)
  - Risk analysis (Section 8.3)
  - Risk evaluation (Section 8.4)
- **Output:** This involves a list of assessed risks prioritized according to the risk evaluation criteria.

Risk assessment in ISO 27005 is a sequence of activities that help an organization identify risks and determine their potential impact. Each step builds upon the previous one to produce the prioritized list of risks the organization will address.

The following presents the three stages of the ISO 27005 process workflow:

Figure 11: ISO 27005 Process Workflow

- **Risk Identification**

Risk identification determines what could happen to cause a potential loss and helps provide insight into how, where, and why the loss might occur. Identification evaluates assets, threats, existing controls, vulnerabilities, and consequences to create a list of incident scenarios that have consequences mapped to assets and business processes.

- **Risk Analysis**
  - Risk analysis produces a list of risks with their value levels assigned by taking output from the risk identification as input for the following three assessments:
  - Assessment of consequences: Assets identified during the risk identification process are valued to produce a list of potential consequences of an incident

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

scenario expressed with respect to assets and impact criteria.

- Assessment of incident likelihood: The organization assesses the likelihood and frequency of events (quantitative or qualitative) to estimate potential impacts.
- Level of risk determination: Output from the first two assessments allow the organization to assign values that communicate the results of risk analysis to support organizational decisions.

The following table provides a sample of a risk scale from 0–8 by mapping likelihood to business impact and then generating a score.

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Table 6: Risk Score Matrix

- **Risk Evaluation:** Risk evaluation combines the list of risks with value levels assigned from the risk analysis phase, the risk evaluation criteria from the context establishment phase, and the risk acceptance criteria defined by the organization to complete the risk assessment process. This produces a prioritized list of risks with two crucial factors:
  - Information security properties: If a criterion is irrelevant for the organization, such as loss of availability, then risks related to this asset may not be irrelevant.
  - The importance of the business process or activity supported by a particular asset or set of assets: If the process is of low importance, risks associated with it should be given a lower consideration than risks that impact more important processes or business activities.

6.13.4. Risk Treatment

The prioritized set of risks produced during the risk assessment supports decisions for the risk treatment plan developed as part of the risk management workflow in ISO 25005. Risk treatment aims to manage organizational risks to an acceptable level. The high-level steps are:

- Review prioritized list from the risk assessment.
- Verify that the risk assessment results are accurate.
- Develop recommendations for risk treatment.

External factors can lead an organization to select specific controls regardless of the assessment results. Some control selections occur because of compliance or contractual obligations. Industry standards and expectations can also result in the selection of specific controls. Due care, the degree exercised under the same or similar circumstances, can create an expectation that a particular type of control exists because of the general adoption of the control within an industry or sector.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.13.5. Risk Acceptance

Risk acceptance typically occurs after risk treatment and validation of control effectiveness. Risk acceptance occurs after risk treatment in the ISO 27005 risk management workflow. The decision to accept the risks and responsibilities for the decision should be made by asset owners and formally recorded following ISO 27001. Risk acceptance produces a list of risks with approved risk treatment plans, approved residual risk, documented deviations from recommendations, and approvals (including budget approval) for completing the work required by the risk treatment plan.

6.13.6. Risk Feedback

ISO 27005 identifies risk monitoring (and review) and risk communication (and consultation) as the two feedback loops that complete the risk management workflow. Each is integral to a successful risk management program.

There are two feedback loops built into the ISO 27005 risk management process. The first is Risk Communication and Consultation, and the second is Risk Monitoring and Review. These two feedback loops are integral to a successful overall risk management program. However, the second, Risk Monitoring and Review, is optional for a one-off risk assessment. An example is a risk assessment as part of a third-party due diligence activity where the assessed third-party may or may not be chosen to become a business partner.

6.13.7. Risk Communication and Consultation

Communication is essential throughout the risk management process. This includes the outcome of assessments, risk status reporting, and analysis of current issues and concerns within the business. A risk communication plan should include insight into the evolving nature of the risks influencing the risk treatment strategy. Formal communication can be used to enhance risk understanding and enable consultation. For example, kickoff meetings at the beginning of a risk assessment project or a risk acceptance meeting at the end of an assessment can provide organizational risk communication opportunities. Risk communication improves risk management practices and can reinforce an understanding of the benefits of the information security risk management program.

It is crucial that during the risk assessment, communication regarding status, issues, concerns, roadblocks, and critical risks that are discovered be rapidly provided to stakeholders and business leaders who will be making risk decisions.

Keeping lines of communication open between the CISO, risk assessment team, and business decision-makers, increases the likelihood that the final risk acceptance will proceed correctly. The risk acceptance phase of the risk assessment should be a mere formality. This communication needs to be open with a risk assessment result that ultimately benefits the organization.

Throughout the process and after the first risk assessment, there should be regular communication to facilitate risk awareness and to provide expectations of potential reassessment of risk. This establishes a culture of continuous improvement within the risk management program.

According to ISO 27005, risk communication should be used for:

- Assuring the outcome of the organization's risk management program.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Collecting risk information.
- Sharing the results from the risk assessment and presenting the risk treatment plan.
- Avoiding or reducing both the occurrence and consequence of information security breaches due to the lack of mutual understanding among decision-makers and stakeholders.
- Supporting decision making.
- Obtaining new information security knowledge.
- Coordinating with other parties and planning responses to reduce the consequences of an incident.
- Providing decision-makers and stakeholders a sense of responsibility for risks.
- Improving risk awareness.

Communication improves risk management practices at the organizational level, assuring benefits are maximized, and corporate dislocation (or dissolution) due to identified risk is minimized. The risk assessment team needs to be responsible for successful risk identification. The program must be connected to the organization's leadership and provide senior management with a clear understanding of the program to garner process support. This will also enable the organization to embrace the risk program results as a relevant business function integrated into the organization's operations.

6.13.8. Risk Monitoring and Review

There are two goals of this feedback loop. The first is to monitor the actual risks and reassess when threats significantly change. The second is to assess and review the risk management program and processes to continuously improve the program and results of the risk management activity in support of organizational goals.

6.13.9. Risk Monitoring

Anything affecting an organization can change the risk posture. Risk inherently changes over time. Threats may change, vulnerabilities can be introduced into systems, vendors release patches, and controls degrade. These can result in increasing the likelihood of risk realization. The environment changes as people, processes, and technology are added or retired. Legacy controls can be forgotten or not appropriately performed. These variables highlight the importance of risk monitoring and review as part of the risk management program. To have an effective risk management program, it is essential to remain engaged with the changing risk landscape and manage and respond to change.

ISO 27005 Risk Monitoring

Organizations should ensure that the following conditions are continually monitored:

- New assets that have been included in the risk management scope.
- Modification of asset values.
- New threats that could be active both outside and inside the organization.
- New or increased vulnerabilities that could allow threats to exploit them.
- Increased impact or consequences of assessed threats, vulnerabilities, and risks in

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

aggregation that can result in an unacceptable level of risk.

- Information security incidents.

6.14. NIST Risk Management Framework (RMF)

The NIST Risk Management Framework (RMF), described in NIST Special Publication 800-37 R2 [7], provides a flexible, holistic, and repeatable 7-step process to manage security and privacy risk and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA). The NIST RMF defines a life cycle for risk management that combines a variety of NIST standards and guidelines to provide an approach an organization can use to manage risk.

The NIST RMF provides the ability to select security controls for federal information systems following the security requirements defined by the Federal Information Processing Standard (FIPS) 200. These requirements are mandatory for U.S. Federal and commercial organizations conducting business on behalf of the U.S. government. Other organizations have the option to use the RMF to define strategies for managing risks.

The risk-based approach of the NIST RMF helps an organization:

- **Prepare** for risk management through essential activities critical to design and implementation of a risk management program.
- **Categorize** systems and information based on an impact analysis.
- **Select** a set of the NIST SP 800-53 controls to protect the system based on NIST SP 800-30 Rev. 1 risk assessments.
- **Implement** the controls, and document how the controls are deployed.
- **Assess** the control implementation to determine if the controls are in place, operating as intended, and producing the desired results to manage risk.
- **Authorize** the system to operate by a senior-level official that understands the controls in place to manage risk and any residual risk.
- Continuously **Monitor** control implementation and changes to the risks to the system.

hide01.ir

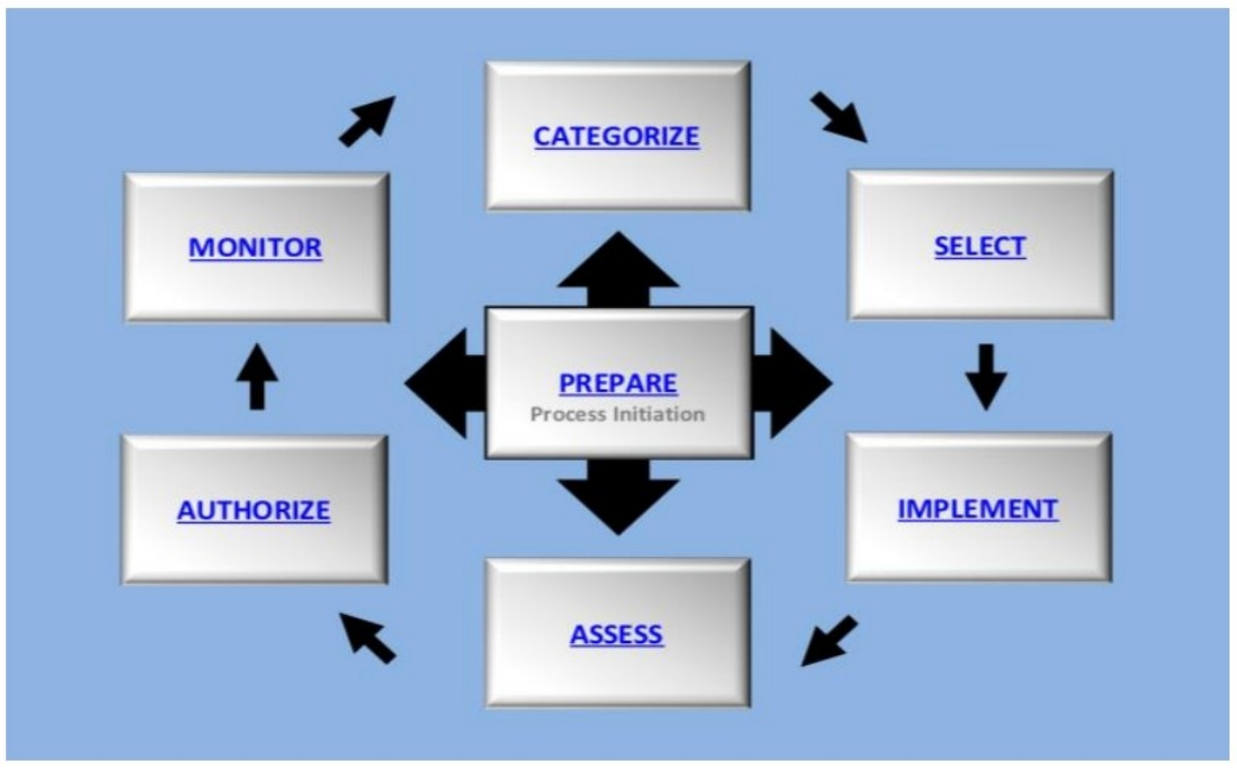


Figure 12: NIST Risk Management Framework (RMF)

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.14.1. Step 1: Prepare

The Prepare step is the first of the RMF process. This means the organization will complete the Prepare step tasks before the Categorize step and support all subsequent RMF steps. The Prepare step is one of the fundamental changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes.

The purpose of the Prepare step is to conduct essential activities at the organization, mission and business process, and information system levels to help prepare the organization to manage its security and privacy risks using the RMF.

The intention is to provide the information and resources necessary to manage the organization's security and privacy risk.

6.14.2. Step 2: Categorize the Information System

The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to the loss of confidentiality, integrity, and availability of corporate systems, administrative operations, and assets, individuals, other organizations, and the nation with respect and the information processed, stored, and transmitted by those systems.

The categorization step uses the catalog of federal information types defined in NIST SP 800-60 to identify the security rating of the system, process, or service. NIST uses a concept known as the high watermark that assigns security ratings based on the highest security rating of data stored, processed, or transmitted by the system. For example, if the system processes one piece of data with a moderate rating, the entire system has a moderate rating. If a system processes moderate- and high-rated data, the system is classified as high.

The categorization process incorporates the definition of the qualitative impact as low, moderate, and high ratings to help the organization understand the risk management strategy used to protect the system.

6.14.3. Step 3: Select Security Controls

The Select step aims to select, tailor, and document the controls necessary to protect the information system and organization commensurate with the risk to organizational operations and assets, individuals, other organizations, and the nation.

The organization uses the combination of FIPS 200 and NIST SP 800-53 to identify controls based on the security rating defined in the Categorization step. FIPS 200 defines the minimum requirements for securing federal information systems. These standards map the security expectations to the categorization of the system. NIST SP 800-53 provides a control catalog from which the organization can select security controls associated with the categorization of the information system.

6.14.4. Step 4: Implement Security Controls

The purpose of the Implement Step is to implement the controls in the security and privacy plans for the system and the organization and to document the specific details of the control implementation in a baseline configuration.

The NIST SP 800-53 controls catalog defines the process for applying controls to the system. It provides a comprehensive approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

fundamentally strengthen their information systems and the environments in which those systems operate, creating more resilient systems against cyberattacks and other threats.

6.14.5. Step 5: Assess the Information System

The Assess step aims to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome for meeting the security and privacy requirements for the system and the organization.

The assessment phase of the NIST RMF provides an opportunity for the organization to evaluate the effectiveness of controls applied within an environment. NIST SP 800-53A provides guidance that helps an organization determine how to implement controls correctly, verify they operate as intended, and produce the desired outcome regarding meeting the system's security requirements.

6.14.6. Step 6: Authorize the Information System

The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk, including supply chain risk, to corporate operations and assets, individuals, other organizations, or the nation based on the function of a system, or the use of standard controls is acceptable.

The authorization phase of the NIST RMF uses output from audits in the assessment phase to develop a list of weaknesses that remain after controls have been applied. This list of weaknesses and the proposed remediation plan create a Plan of Action and Milestones (POAM) that reflects the organization's priorities regarding remediation of findings from the assessment. Suppose the organization determines the POAM is acceptable. In that case, an organizational leader with the role of Designated Approval Authority (DAA) or Designated Authorizing Official (DAO) accepts the residual risk associated with the system's operation and allows its deployment.

hide01.ir

6.14.7. Step 7: Monitor Security Controls

The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

Monitoring is the final phase of the NIST RMF. Monitoring provides ongoing evaluation of existing controls and processes to ensure controls remain effective as the system undergoes life cycle changes and modifications. The organization defines a time limit for periodic reassessment as part of the monitoring process. This assures that controls evaluated at the beginning of the NIST RMF cycle remain relevant throughout the system lifecycle.

This process also provides an essential opportunity for assurance that weaknesses identified for remediation in the Plan of Action and Milestones (POAM) are managed. In addition, the process ensures new weaknesses identified in the system are managed.

6.15. NIST Risk Management and Assessment

The guidance described in SP 800-37 for applying the RMF to federal information systems does not include the risk assessment process. Guidance for conducting risk assessments is documented in NIST SP 800-30 [6], and additional risk management guidance is written in NIST SP 800-39. These documents help organizations go beyond the qualitative assessment outlined in the NIST RMF and perform a more comprehensive review and management of risks.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.16. NIST Risk Management Hierarchy

Assessing risk is a fundamental component of the risk management process. A risk management process, illustrated in the below figure: NIST RMF Hierarchy, consists of framing the context of risk, assessing risk, responding to risk, and monitoring risk.

The first component of the process is the frame, which establishes the context of risk by describing the environment and constraints against which risk-based decisions will be made. The frame guides how organizations assess, respond, and monitor risks. Input to the risk assessment component includes an organization's threats and vulnerabilities. The outcome is the projection of potential impacts and likelihoods. The response component determines how risk is treated. The monitor component provides the continuous evaluation of the risk.

The following is the NIST hierarchy model:

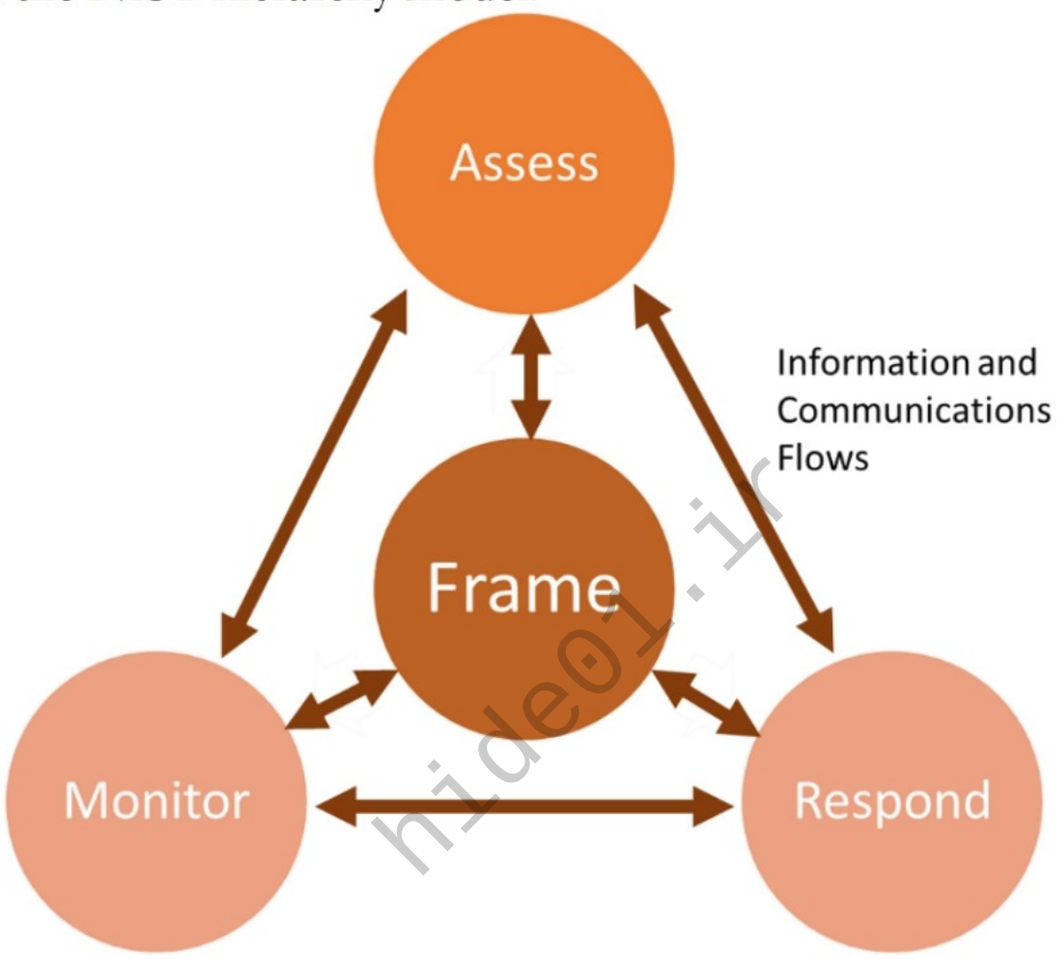


Figure 13: NIST RMF Hierarchy

NIST SP 800-30 describes assessing information security risk in support of the goals defined in NIST SP 800-37 and NIST SP 800-39. This risk assessment process includes four steps that help an organization understand its risks.

6.17. NIST Risk Assessment Process

Step 1: Prepare for Assessment

This first step is critical to the overall context and success of your risk assessment—and, therefore, your entire risk management. Preparation is heavily influenced and shaped by the framing stage of your risk management.

To prepare for a full-fledged risk assessment, you need to:

- Identify purpose for the assessment.
- Identify scope of the assessment.
- Identify assumptions and constraints to use.
- Identify sources of information (inputs).

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify risk model and analytic approach to use.

Step 2: Conduct Assessment

This step is the focus of the entire risk assessment process; it entails putting your plan into action. This step produces a list of information security risks that can be prioritized by risk level and is used to support risk response decisions. The assessment comprises two main sub-processes.

The first is further identification, and the second involves analysis of data uncovered:

- **Identification** – You need to define what threats exist, their sources, and what potential events could occur because of vulnerabilities being exploited.
- **Determination** – Once you have identified the threats, you need to determine all possible negative impacts they could have on all parties involved and the relative likelihood of each scenario.

Step 3: Communicate Results

This step entails gathering the information from the assessment and communicating it to all parties impacted by the risks and scenarios plotted. Communication and sharing help distribute information developed in the execution of the risk assessment.

This stage is the same for all organizations undertaking it, with the caveat that significant differences in the scope and scale of the company and the risk assessment are reflected in how this stage functions.

This step assures that decision-makers have the necessary risk-related information to guide risk decisions.

Step 4: Maintain Assessment

The final part of the NIST risk assessment process entails setting yourself up for continued, ongoing assessment over the long term. This stage comprises a combination of detailed monitoring of all previously identified risk factors and scanning for new ones. This step supports the continual review of risk management.

In addition, you also need to constantly update your communication and other risk management practices based on new findings. Assessment must not be an isolated, one-time occurrence. Instead, it must be an element of your company's overall culture.

The following figure presents the NIST risk assessment process:

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

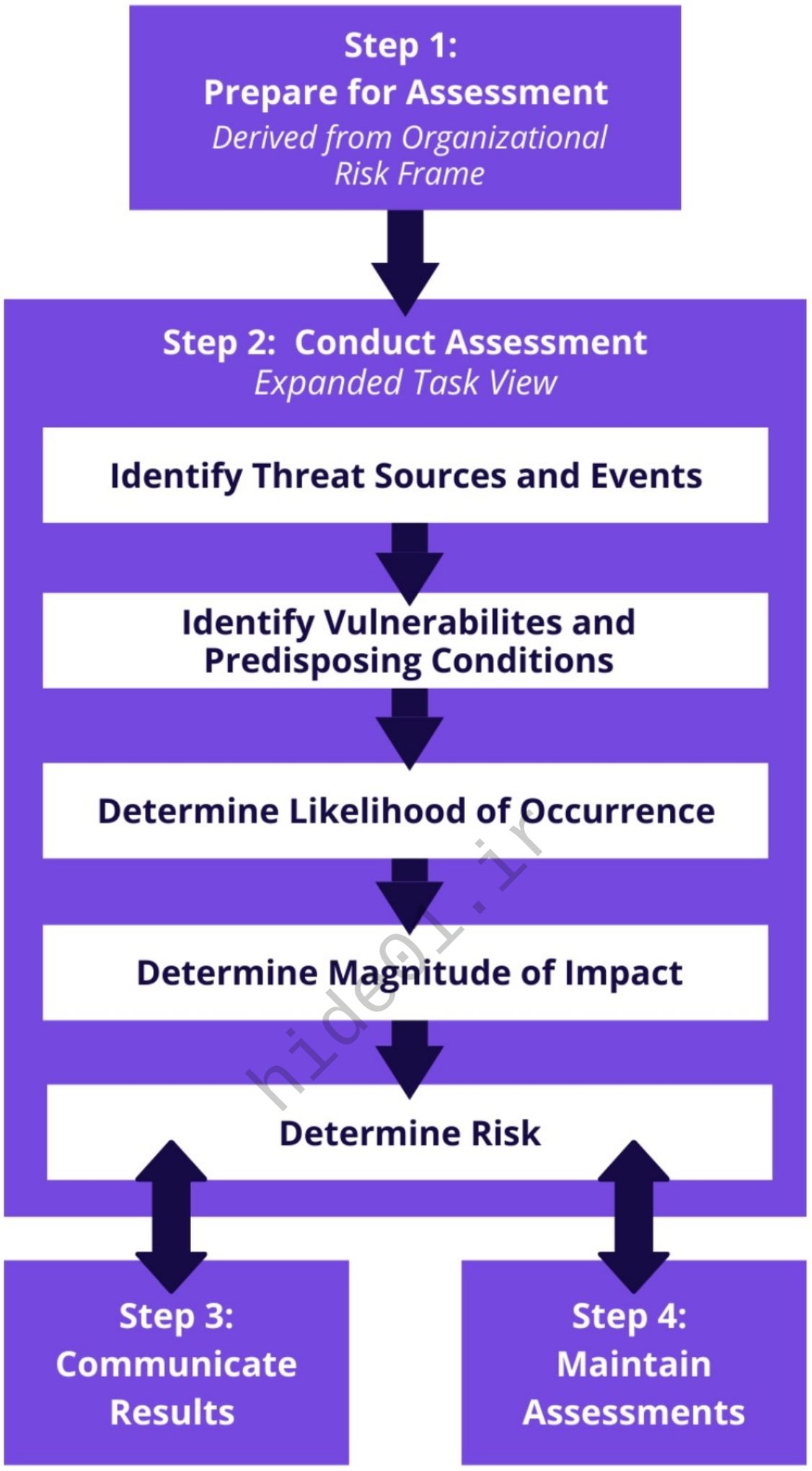


Figure 14: NIST Risk Assessment Process

6.18. Other Frameworks

Although ISO 27005 and the NIST RMF are the most common frameworks available to support information security risk management, other approaches exist that can replace or supplement these approaches.

6.18.1. COBIT Risk Management

Control Objectives for Information and Related Technology (COBIT) is an ISACA framework for IT management and IT governance that can be used to support information security risk management. COBIT consists of linking business goals to IT goals, providing

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

metrics and maturity models to measure their achievement, and identifying the responsibilities of business and IT process owners. COBIT 5 consolidates and integrates COBIT 4.1, Val IT 2.0, and Risk IT frameworks. It also uses ISACA's IT Assurance Framework (ITAF) and the Business Model for Information Security (BMIS) to define sound risk management practices.

6.18.2. COSO Enterprise Risk Management Integrated Framework

The COSO framework, first published in 1994, defines Enterprise Risk Management (ERM) as a "…process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." [13]

The COSO ERM Framework itself is a set of principles organized into five interrelated components:

- Governance and Culture: Governance sets the organization's tone, reinforcing the importance of and establishing oversight responsibilities for enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
- Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in strategic planning. A risk appetite is established and aligned with strategy; business objectives put the plan into practice while serving as a basis for identifying, assessing, and responding to risk.
- Performance: Risks that may impact the achievement of strategy and business objectives must be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
- Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components function over time, considering substantial changes, and what revisions are needed.
- Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing information from internal and external sources, which flows up, down, and across the organization.

The current release of COSO was published in 2017.

6.18.3. Information Technology Infrastructure Library (ITIL)

ITIL is an acceptable solution to support information security risk management. Formerly known as the Information Technology Infrastructure Library, ITIL is a set of practices for IT service management that focuses on aligning IT services with the needs of a business. Because business alignment is a security goal, a CISO can leverage mature IT service delivery practices to provide information security services to the organization. ITIL's Service Operation (SO) processes are beneficial to support security objectives by outlining best practices for delivering value regarding event management, identity management, problem management, and incident management processes.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.18.4. Factor Analysis of Information Risk (FAIR)

FAIR is a tool that complements existing risk management frameworks by providing a model to understand, analyze, and quantify information risk in financial terms [14]. FAIR's risk model components are specifically designed to support quantitative risk management.

The following presents the FAIR risk model:

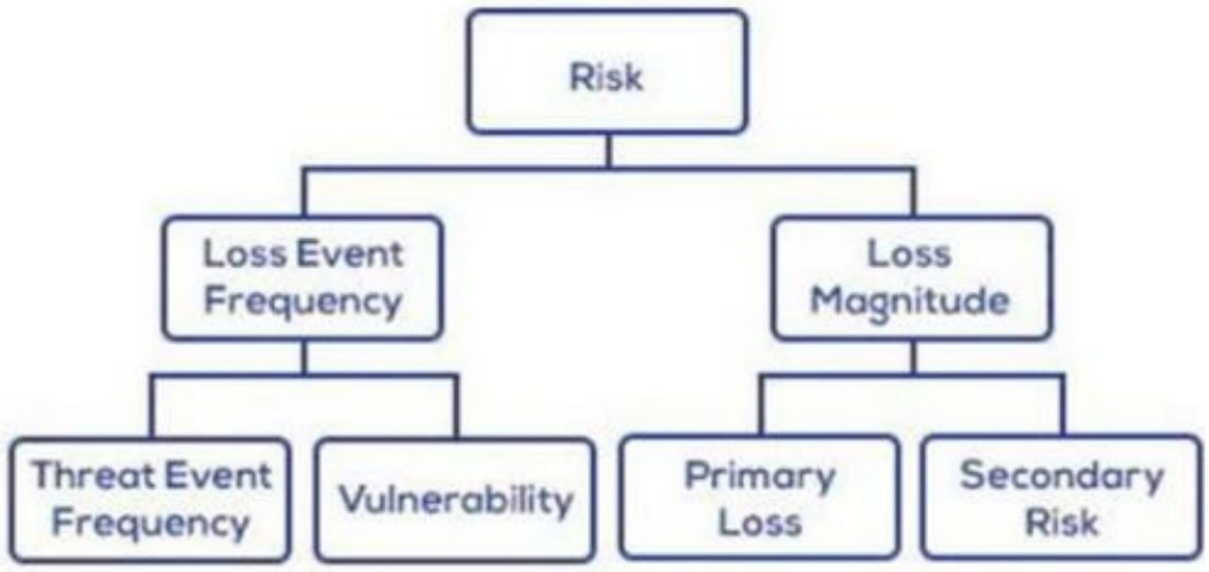


Figure 15: FAIR Risk Model

FAIR selects at least one object within an environment and quantifies the strength of its controls. This is done by quantifying authentication controls, authorization controls, and structural integrity. Next, global variables are set up for the environment. For example, a determination is made as to whether the environment is subject to regulatory laws. Then, selecting at least one threat community, information risk is calculated.

This calculation is accomplished by performing a statistical analysis using the strengths of controls on at least one object, the characteristics of at least one threat community, and the global variables of the environment. This is used to compute a value representing information risk.

The method identifies the salient objects within a risk environment. It defines their characteristics, considering how they interact with each other. FAIR derives probabilities using a statistically sound mathematical calculation to emulate these interactions. The method then represents the security risk as an integer, distribution, or other variable [15].

6.18.5. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE Allegro is a lean risk assessment method that does not guide selecting security controls. The framework supports a simple qualitative risk assessment and a structured threat analysis, primarily suitable for smaller organizations [16]. Also see the OCTAVE Allegro Roadmap [16].

OCTAVE Allegro consists of eight steps organized into four phases. The framework allows an organization to focus on the most critical assets by ensuring they are selected for review through a systematic and consistent process. The organization can better define a manageable scope by concentrating on information assets exclusively and other assets (such as people, technology, and facilities) through association with information assets. This reduces the effort required for threat identification, risk analysis, and mitigation planning. The phases are summarized as:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Develop risk measurement criteria consistent with the organization's mission, goal objectives, and critical success factors.
- Create a profile of each critical information asset that establishes clear boundaries for the asset, identifies its security requirements, and identifies its containers.
- Identify threats to each information asset in the context of its containers.
- Identify and analyze risks to information assets and develop mitigation approaches.

The following presents the OCTAVE framework workflow steps:

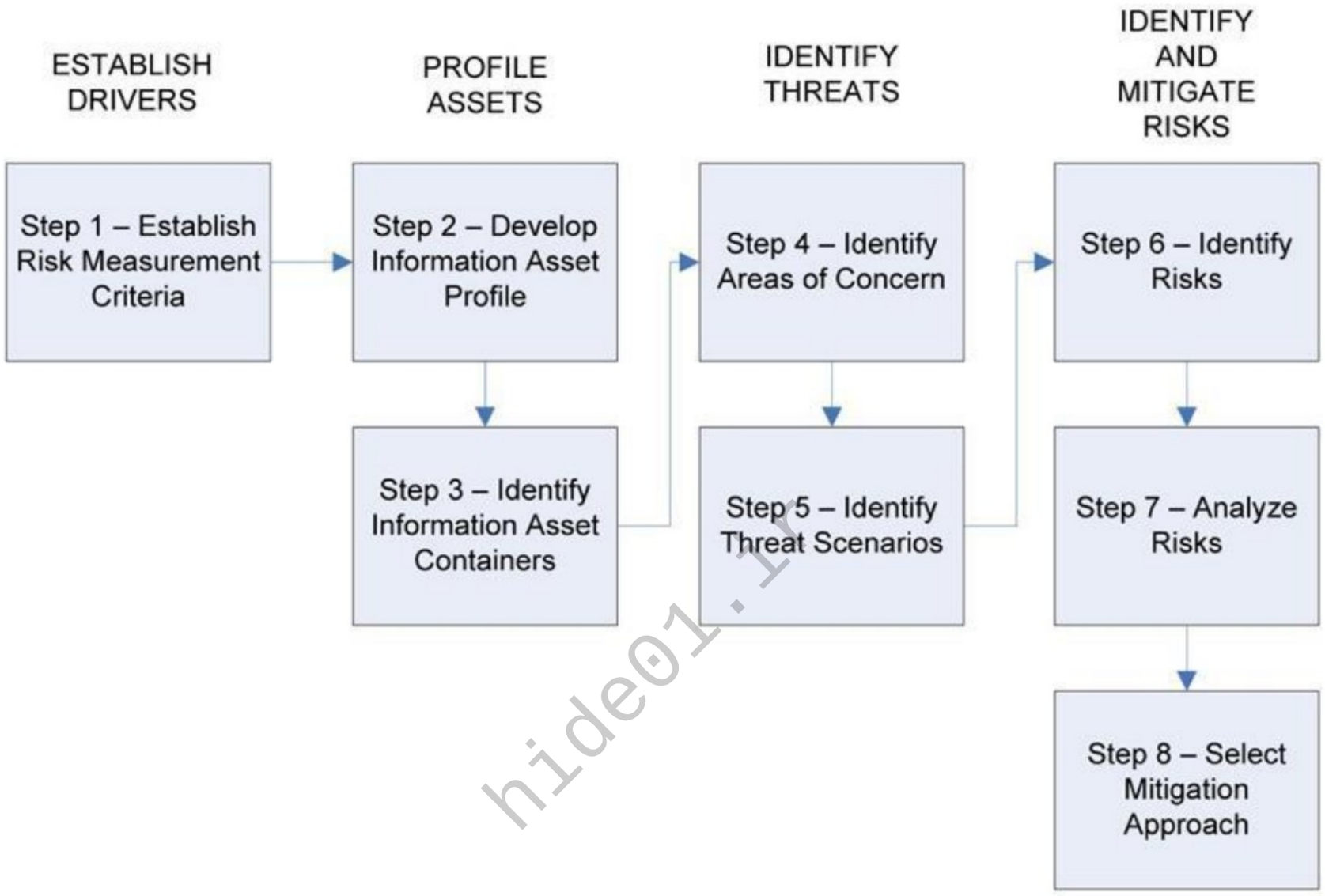


Figure 16: OCTAVE Framework Workflow

6.18.6. Threat Agent Risk Assessment (TARA)

TARA distills the immense number of information security attacks into a digest of only those exposures most likely to occur to support the development of optimal security strategies [17]. TARA identifies threat agents pursuing obtainable objectives that could cause unsatisfactory losses. The approach concentrates on threat agents and their motivations, attack methods, attack objectives, and how they map to existing controls. It does not focus on weak points associated with specific vulnerabilities.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

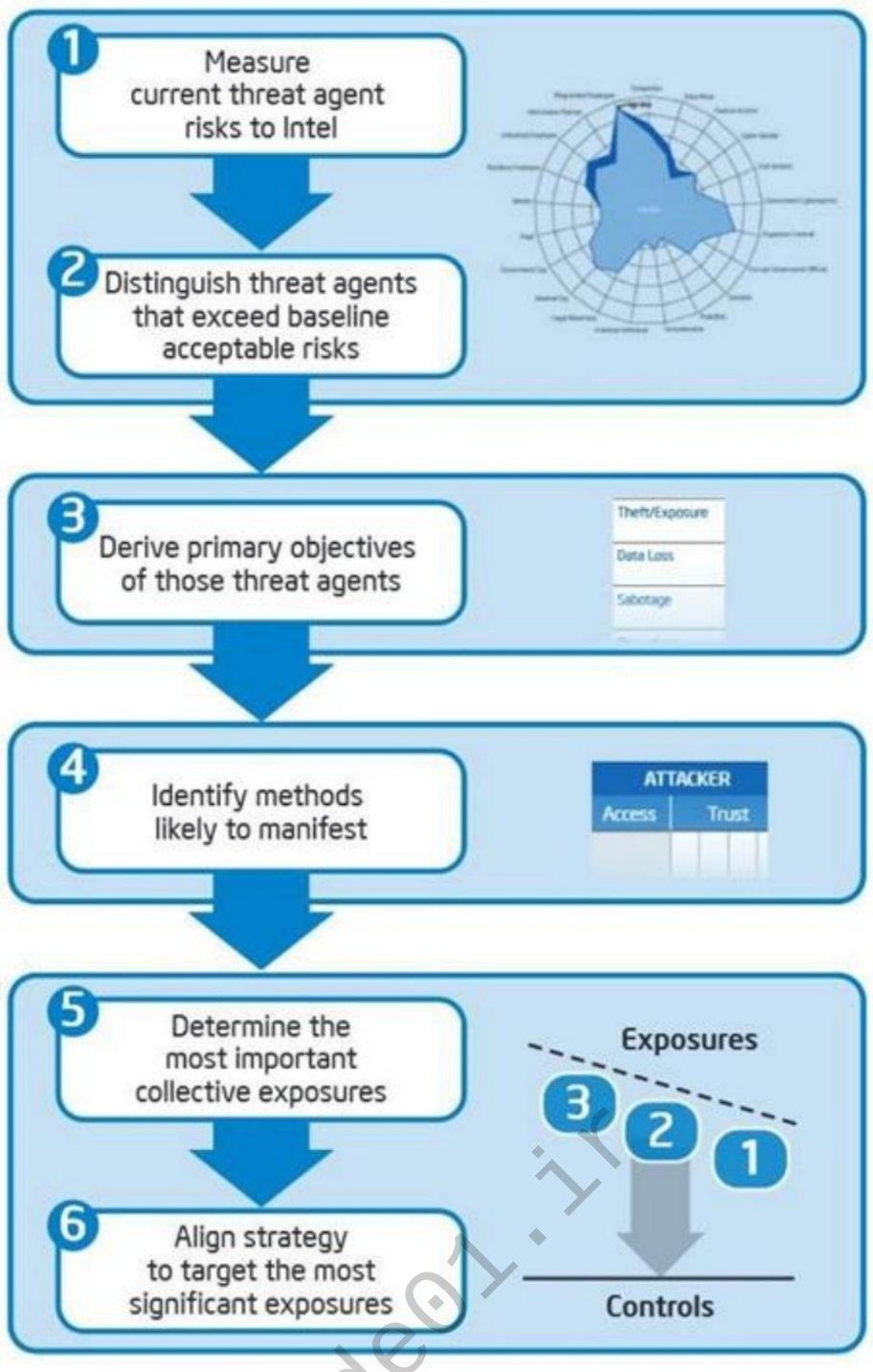


Figure 17: TARA Methodology

6.19. Risk Management Policies and Procedures

For a well-managed, repeatable risk management program, it is critical to document these activities in policy, standards, procedures, work instructions, and guidelines (or some subset). There is a hierarchy to these documents, and all of these should align with the chosen risk management framework for the organization (such as ISO 27005, ISO 31000, COBIT, NIST 800- 30/37/39, and OCTAVE).

The policy should provide the overall direction and purpose of performing risk management. In effect, the organization intends to perform risk management. Within the policy, it is helpful to articulate responsibility for the program and to appoint a business owner for risk management. This business owner should be the owner of the policy and will be the senior authority within the organization regarding risk management and should be the senior executive sponsor who will provide the high-level cover and formal liaison with the CEO, other senior executives, and the board (and if it exists, the risk committee of the board of directors).

The policy should conform to the documentation standard for policies within the organization and include all the typical boilerplate language for organizational policies. This typically will consist of the following sections:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A. Section devoted to document management indicating

a. The subject of the policy
b. Sequence number (if used by the organization)
c. Effectiveness date
d. Author
e. Contributor(s), if any exist
f. Approvals
g. Change record (including versioning, dates of changes, and a brief description of the change)

B. The purpose of the policy

a. Reason for the policy to exist — To appropriately manage organizational risk systematically
b. Mention of the organization — For Organization X
c. Some shorthand for the organization's name (such as "company" or "organization") so that it is not necessary to repeat the name throughout the document repeatedly

C. The policy itself

a. Approach
b. Scope and boundaries (systems, locations, departments, organization)
c. Organization responsible for performing the activities
d. The requirements outlined in any framework or methodology
e. Requirement for continuous improvement

D. Breach of policy and enforcement

a. Clear statement of ramifications for not following the policy
b. Can be a reference to a Sanctions policy or equivalent

E. Applicability of the policy

a. Who is covered by the policy/who the policy applies

F. References

a. Compliance requirements
b. Framework documents
c. Other policies

The policy will provide the overall guidance for the risk management program and will provide the necessary political cover at the senior executive level to perform the activities outlined in the policy. The policy will also guide the operational documents, standards, and procedures. In the case of a risk management program, the standard procedure is often known as the risk management or risk assessment manual. This manual contains the formal documentation and procedures per the described standard. Occasionally, even the policy is included in the risk

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

management manual. However, by placing the policy within the manual, the rest of the organization will lose sight of it in the larger collection of policies since it will have disappeared into something that is not called a "policy."

When it comes to the risk management manual, the included standard(s) and procedure(s) describe first what needs to be done to meet the requirements of the risk management policy (this is the standard) and then how to perform that activity (this is the procedure). As was outlined earlier in this domain, each step of the risk assessment activity needs to be clearly documented within the risk management manual. It is here where all the process improvements will be documented as updated procedures to improve the practice of risk assessments within the organization continuously.

Is it necessary to do all this documentation and align it to a framework, create a policy, and document standards and procedures? Ideally, yes, as this activity informs a continuous improvement culture. If accurate documentation is not maintained, every time the organization requires a risk assessment, the team doing the work might be reinventing the process, and improvement may not be built into the program. As the information security leader of the organization, the CISO must be effectively the cheerleader for documentation and formalizing processes and making continuous improvement and excellence in results in the program. This will lead to greater maturity, improved outcomes, and enhanced prestige within the organization for delivering a risk management program that is clear, business-focused, aligned to organizational success, and continuously improving to assist the organization in driving down adverse outcomes cost-effectively.

6.20. Risk Management Lifecycle

An effective risk management program includes an articulated lifecycle ensuring that risk is managed continuously and methodically. The below figure shows the typical cyber risk management lifecycle.

hide01.ir

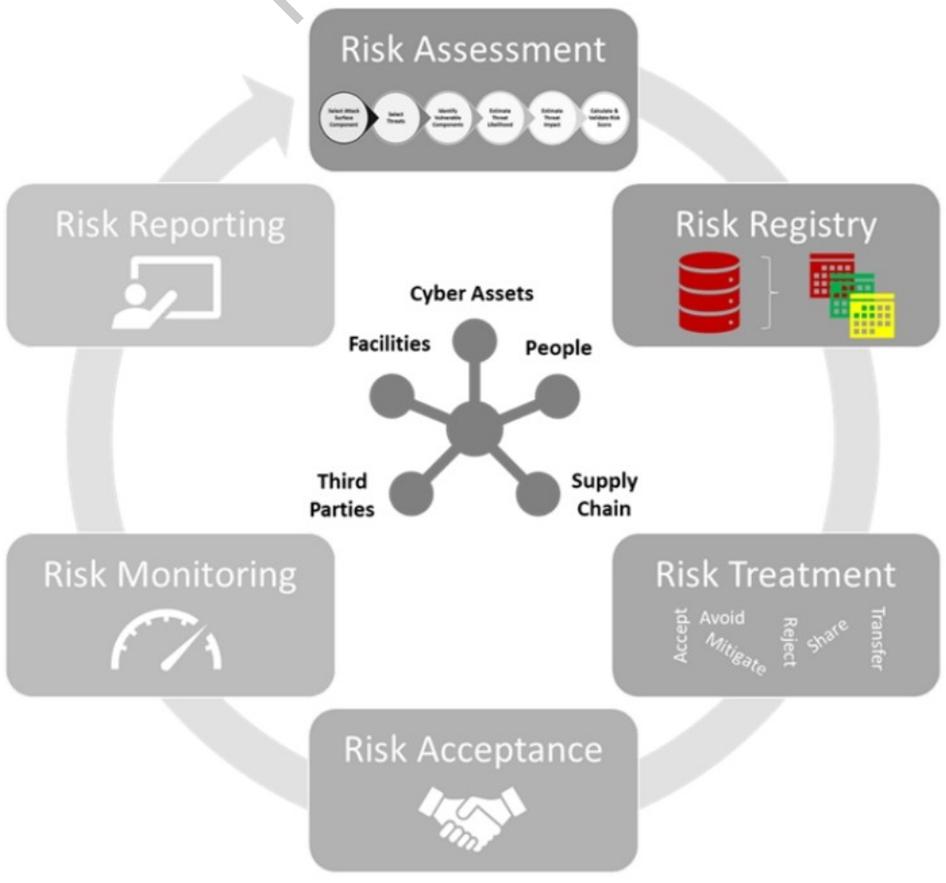


Figure 18: Risk Management Lifecycle. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License)

The following describes each component of the model:

- **Risk Assessment:** The lifecycle begins with performing risk assessments that will

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

determine quantitatively or qualitatively the risk between a relationship of threats, vulnerabilities, and attack surface components. The determination of risk is a product of the likelihood a threat can exploit a vulnerability and the ensuing degree of compromise. Risk assessments should have a defined shelf-life because the attack surface changes, threat profiles change, and the exploit tools used by threat actors change. Your higher-risk-rated applications, for example, should be reviewed annually. In contrast, lower-risk computing equipment may be risk-reviewed every 24 to 36 months, depending on the complexity of your attack surface components. There are three primary categories of risk assessments:

- **Qualitative Assessments** – This approach uses numbers to identify the degree of risk an organization would face. Risk assessment results are based on facts and figures.
- **Quantitative Assessments** – This approach uses interpretations and observations to dimension an organization's risk. Risk assessment results are descriptive and subjective.
- **Hybrid Assessments** – This approach uses qualitative and quantitative methods to present the state of risk of an organization.

- **Risk Registry**: Once assessments are completed, they must be stored in a central repository for continuous management. Each risk registered adds to the inventory of risks that may be assigned to other applications, software, hardware, or networking devices. The registry is the hub of the risk management workflow, where risks and risk treatments are regularly reviewed. Change control is an integral aspect of the registry, with each action to manage risk well documented.
- **Risk Treatment**: Risks entered in the registry are considered untreated until they are assigned a risk treatment plan. The treatment plan can range from simply accepting the risk to applying layers of sophisticated countermeasures. Regardless of the treatment plan complexity, your highest-rated risks must be addressed first. The treatment plan elevates the inherent risk score to a treated risk score. What is left is residual risk. Treatment plans may require improvement based on audits, regulatory control advances, or threat landscape changes.
- **Risk Acceptance**: Accepting risk is much more than saying you accept it. Acceptance requires a formal written declaration by senior management that your organization understands the consequences and that a conscious decision was made that no further risk treatment can be made. Risk acceptance must also be communicated to any entity impacted by the decision to accept this risk. You may have to issue a risk waiver when a risk owner cannot comply with the risk treatment plan. This is considered risk acceptance.
- **Risk Monitoring**: Risk management must be transparent, tracking and reporting risk to stakeholders. Monitoring is a closed-loop approach where risks are tracked from identification to implementing their treatment plans. An essential aspect of monitoring is tracking risks that have occurred. Risk treatment plans do not guarantee that a risk will never materialize. Each time a risk event occurs, a postmortem of the treatment plan is required.
- **Risk Reporting**: Timely and accurate risk reporting is integral to your risk management capability. Communicating your organization's risk profile to the right audience raises risk awareness and moves you toward a risk-aware culture. Risk reporting can range from self-

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

serve dashboarding to publishing risk reports. Utilizing a set of well-thought-out cyber risk metrics will increase the effectiveness of your risk reporting.

6.21. Risk Management Program Implementation Use Case

For this section, ISO 27005 will be used as a use case or guidance on deploying a complete risk management program.

Let us discuss when and how to perform a risk assessment. Risk assessments should be performed as frequently as necessary. Times when risk assessments are necessary include:

- When setting a baseline for an organization. This is the time to discern the risks, how they should be treated, and to get management's approval of the risk treatment plan.
    - As part of any new project, in other words, a project risk assessment includes information security and project risks (risks to the project's schedule and deliverables).
    - As part of the due diligence process for acquiring new services or solutions (this is also known as third-party due diligence).
- As required within any mandatory compliance framework (HIPAA, PCI DSS, ISO 27001, and National Security frameworks/standards).
- Anytime something significant changes within the environment, including:
    - The threat landscape changes.
    - New vulnerabilities are detected.
    - Assets change or the value of assets change.
- As part of a reassessment program—typically, this is combined with the significant change review step mentioned above, as the reason for these reassessments is to catch anything that might have changed. This can also be combined with existing procedures requiring annual reassessment of risks. In any case, reassessment of risk should occur on a schedule that helps the organization meet the risk mitigation goals and risk tolerance—usually as noted in the risk management policy or program documentation.

hide01.ir

Step 1 – Identification of Assets

The easy part of this identification of assets is hardware and software. If there is an asset inventory, this list of hardware and software should be listed there. However, assets that have value include much more than physical assets. They include the data residing on systems as well as business processes. ISO 27005 considers "primary assets" as:

- Business processes and activities
- Information

Most of the time, people think of assets as being the physical devices and infrastructure. However, organizational dynamics and the information required to operate the company can have significantly more value than the physical systems (computers, networks, etc.) needed for the business process, activities, and the information stored on those physical systems. ISO 27005 considers those physical systems to be supporting assets, and these supporting assets include:

- Hardware

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Software
- Network
- Personnel
- Site
- Organization's structure

These supporting assets are important because primary assets require them for use by the organization. Remember that information regarding all supporting assets must also be protected from an external threat to access a primary asset. It is possible for a threat to access the network and compromise a system to access data stored on those systems. But it is also possible that the same threat actor could kidnap the key employee, for example, and through intimidation, extortion, or torture, extract information, gaining access to the data on those same systems. The CISO's job is to protect the organization's information, but those assets include people and technical ones. (As an aside, this is one of many arguments to have the information security function sit outside of IT as responsibility extends well beyond protection for technical assets.)

The output for Step 1 includes a list of assets to be risk-managed and a list of business processes related to investments and their relevance. As CISO, the time spent understanding the organization will help provide the required context in this output step and the information necessary to assist the team in determining relevance to the assets and excluding those that are irrelevant to the organization.

Step 2 – Identification of Threats

Now that we know our assets, the next step is to understand the threat to those assets. So, the question is, how do we determine our threats? Well, some are natural events and particular to the assets' location.

In some regions, tornadoes are common and would be a threat. Elsewhere, the prevalent natural disasters include earthquakes, hurricanes, tsunamis, or flooding. Some places have several potential threats caused by Mother Nature. Human-made disasters are more frequent in other areas of the world, including wars or civil unrest, manufactured environmental damage, or even legislative activities with potentially unforeseen consequences. And, of course, there are threats caused by malicious outsiders and insiders (or even unwitting insiders).

Several security companies offer threat monitoring services providing some form of threat detection and/or intelligence. Alternatives to purchasing threat monitoring services to obtain better intelligence on potential threats to a particular location include previous risk assessments (but don't forget to determine whether the threat landscape has changed), coworkers at the company who could give clues to threats (those that have caused incidents in the past as well as those that are suspected of potentially causing incidents in the future), and even the standard or framework in use at the organization. For instance, in ISO 27005 Annex C, there is a list of "examples of typical threats."

From ISO 27005 Annex C, the following table gives examples of typical threats. The list can be used during the threat assessment process and as a starting point in identifying or verifying the identified threats. Threats may be deliberate, accidental, or environmental (natural) and may result, for example, in damage or loss of essential services. The following list indicates each threat type where D (deliberate), A (accidental), and E (environmental) are relevant. D is used for all deliberate

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

actions aimed at information assets, A is used for all human actions that can accidentally damage information assets, and E is used for all incidents not based on human actions. The groups of threats need to be in priority order.

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of Equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Unauthorized actions	Unauthorized use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D

hidee01.ir

Table 7: ISO 27005 Annex C - Examples of Typical Threats

What is essential for a CISO is to validate the threats identified by the assessment team and to guide them in making them relevant. Additionally, the CISO needs to take a strategic perspective and determine if strategic threats are missing. For instance, a CISO may be aware of an impending acquisition deal or an unknown (confidential) pending lawsuit. Adding additional threat context during the assessment may be possible without revealing the details behind the knowledge.

The output for Step 2 is, "A list of threats with the identification of threat type and source."

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 3 – Identification of Existing Controls

The assets and threats we identified in steps 1 and 2 are not inputs for step 3. Instead, the information for step 3 is documentation of controls and risk treatment implementation plans. The purpose of this step is to understand what the organization has already accomplished as the result of previous risk management activities and any controls that have already been implemented. Keep in mind that some controls implemented within many organizations are not the result of a formal risk assessment but are instead implemented for various other reasons (e.g., because peers do it, because it is a generally accepted or know practice, because an auditor or customer required it etc.).

If the CISO already has a good handle on the controls implemented within the organization, the next step is to create a control inventory. Unfortunately, it is common to find controls that have been implemented either for no purpose (mitigating no existing risk) or incorrectly. For example, let us imagine a critical system in the organization where domain administrators have been removed from the administrator group and the local administrator password has been changed. Over time, the users who were members of the local administrator group had their accounts deleted, and now nobody can log in as an administrator. This is an example of a control that was initially designed to reduce the number of administrators on the critical system, which was a good idea. Still, this solution needed to be documented and was implemented incompletely and incorrectly.

ISO 27005 (8.2.4) outlines four activities that are helpful for identifying existing controls:

- Reviewing documents containing information about the controls (e.g., 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.
- Checking with the people responsible for information security (e.g., information security officer, building manager, or operations manager) and the users as to which controls are really implemented for the information process or information system under consideration.
- Conducting an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented as to whether they are operating correctly and effectively.
- Reviewing results of audits.

The purpose of understanding what controls already exist is to ensure that duplication of controls does not occur and that there are no controls implemented that no longer serve a purpose (and are consuming organizational resources). As CISO, removing unnecessary controls (especially controls that have caused some amount of pain within the organization) can be a big win for the information security group. The removal of controls is usually looked upon favorably since the effect often times results in improved operational efficiency.

The output for Step 3 is, "A list of all existing and planned controls, their implementation, and usage status."

Step 4 – Identification of Vulnerabilities

The input for step 4 is "Lists of assets, lists of known threats, and lists of existing controls." We

pide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

now have our list of assets, threats, and controls. The first two steps give us a list of threats that can potentially exploit a vulnerability to our assets, and the third step provides information about whether we have an existing control to mitigate the threat to our critical assets.

Now that we have several of the pieces to this risk assessment puzzle, it is essential to note that "the presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it." Without a threat that can exploit a vulnerability on the other side, "a threat that does not have a corresponding vulnerability may not result in a risk." We have significant pieces of the puzzle to identify risks once we have completed the first four steps. So, how do we determine and identify our vulnerabilities?

From a technology-centric viewpoint, the risk assessment team will identify vulnerabilities by leveraging tools such as vulnerability scanners, web application scanners, source code scanners, database scanners, vulnerability assessments/penetration tests, attack surface management solutions, and more.

Additionally, Annex D of ISO 27005 lists examples of vulnerabilities; these can be used as a step for verifying that vulnerability assessments have been completed comprehensively. Only the hardware and software vulnerabilities from Annex D are noted for illustration purposes. For the extensive list, please refer to the complete document.

Type	Examples of Vulnerabilities	Examples of Threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Susceptibility to temperature variations	Meteorological phenomenon
	Unprotected storage	Theft of media or documents
	Lack of care at disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
	Well-known flaws in the software	Abuse of rights
	No 'logout' when leaving the workstation	Abuse of rights
	Disposal or reuse of storage media without proper erasure	Abuse of rights
	Lack of audit trail	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
	Widely-distributed software	Corruption of data
	Applying application programs to the wrong data in terms of time	Corruption of data
	Complicated user interface	Error in use
	Lack of documentation	Error in use
	Incorrect parameter set up	Error in use
	Incorrect dates	Error in use

hide01.ir

Table 8: ISO 27005 Annex D - Examples of Vulnerabilities

The output for Step 4, according to the ISO 27005 standard, is "A list of vulnerabilities about assets, threats, and controls; a list of vulnerabilities that do not relate to any identified threat for review." This will give us a complete picture of vulnerabilities; however, for the next step, vulnerabilities without any associated threat will not create a risk. They will need to be monitored in the future as a threat may materialize.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 5 – Identification of Consequences

The fifth and final step of the risk identification process is to take the results of the first four steps, "A list of assets, a list of business processes, and a list of threats and vulnerabilities, where appropriate, related to assets and their relevance" and determine the adverse outcome should there be a loss of confidentiality, integrity, or availability (a security incident) as a result of a threat exploiting a vulnerability to one or more assets.

Consequences can be varied. If the organization had an incident, the consequences could be significant. ISO 27001 provides some examples of "operational consequences of incident scenarios":

- Investigation and repair time
- (Work) time lost
- Opportunity lost
- Health and safety
- Financial cost of specific skills to repair the damage
- Image reputation and goodwill

You have likely had to respond to incidents in the past. The reality is that it creates significant dislocation to an organization anytime an incident occurs. Personnel are reassigned from regular duties (generating a cost to the organization while creating value for the organization's incident response effort) to understand what is going on with the incident and perform remediation. Proper root cause analysis and corrective actions take time and effort. Frequently, the personnel assigned to do this work are some of the organization's most capable technical personnel, meaning these high-value assets are spending time doing this work of remediation and not doing work to add value to the organization.

Consequences should a risk event manifest can be pretty dire and quite expensive. Some incidents could cause significant brand damage and damage the organization's relationship with existing and prospective clients. All of this must be captured when evaluating consequences. It is also where a CISO's judgment will potentially be called into question, and that is why it is important to attempt to perform the entire risk assessment and consequence analysis in a systematic, impartial way to reduce or, as much as possible, eliminate the appearance of overreacting as a ploy to garner additional funds.

The output of this last step in the risk identification process is "A list of incident scenarios with their consequences related to assets and business processes."

6.22. Risk Management Program Review

The continuous improvement program is the risk management program's last and arguably most important part. Even if the initial efforts at risk assessment are not first-rate, it is possible to eventually evolve into a world-class risk management operation through continuous improvement.

The first time most organizations do something, it could be better. The first time a new CISO performs a risk assessment, the same is often true. What is learned from those mistakes and the steps taken to improve the risk management program in the future is what matters. The program review and the concept of continuous improvement will lead to improvements over time. They should be embraced by a professional CISO and not be looked upon as criticism (although it can

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

be hard not to take it as such).

To embed continuous improvement during the risk assessment process, select one of the people on the risk assessment team as an observer who can, in an objective way (as much as possible), record their observations and thoughts as the process plays out and as each step in the risk assessment process is completed, have that person submit those findings for the CISO to review. This can be especially important during the first risk assessment exercise as these early reflections upon the process could be forgotten if the team waits until the end of the risk assessment to review what went well and what can be improved.

As a CISO, when reviewing these documented observations, try to determine whether it would be helpful to intervene immediately to impact the risk assessment process as it is being performed or whether it is more prudent or valuable to wait until later in the process or at the end of the risk assessment to provide end of project feedback that will, in turn, be used to improve the following risk assessment.

7. SUMMARY

The central message and essential function of information security involves understanding the risks to the organization and appropriately managing those risks systematically to achieve organizational goals and drive organizational success.

The risk assessment, control selection, control maintenance, and audit/assessment are the basics of information security. As CISO, it is critical to construct the risk management program properly, leveraging frameworks where appropriate. This should be the first task accomplished when building a new information security program. If joining an existing information security team, this is the initial evaluation that should be conducted (also consider partnering with the internal audit function to assess the capability and capacity of the risk management function). The outcome of this audit will allow the CISO to understand the program's weaknesses, correct those weaknesses, and then build the information security program from a solid foundation.

nigeo.ir

Once the risk management function is working appropriately, the next step for a new CISO should be to conduct a risk assessment across the entire organization and entire infrastructure (if possible), evaluate the existing controls, and determine risk treatment to achieve the risk retention goals of the organization. An intimate understanding of Domains 3 and 4 will help develop appropriate controls and place existing controls into a proper context.

When creating a risk treatment plan, it is vital to understand the several types of controls that can be implemented, including the various technical controls noted in Domain 4 and how those controls operate. Automated and manual controls, in combination, provide more risk mitigation than one or the other alone. Policies and procedures have their place, as do technical controls. The reason for discussing the several types of controls is that they can be combined to achieve more significant risk mitigation through precisely choosing the proper management and the correct mechanism of implementation and maintenance of the control. By blending several types of controls, risk should be further reduced.

Once the controls are implemented, assessing, and verifying that the controls are operating effectively is necessary. Thus, the CISO must implement a methodology for validating control effectiveness through the assessment/audit topics discussed in Domain 2, tracking appropriate metrics, and, where possible, automating controls. A perfectly designed manual control requiring a fallible human to spend

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

substantial portions of their day performing a repetitive task in the hopes of finding the proverbial needle in a haystack will not operate perfectly in real life. Appropriate assessments and metrics would make clear the ineffectiveness of that scenario.

If the metrics do not demonstrate the futility of incredibly dull repetitive tasks, a well-conceived and independent audit function would note the failing and make appropriate recommendations to remedy the manual control failure (and replace it with an automated control performed by a computing device that never grows bored).

This domain is information security at its essential essence—understanding risks and placing them into a governance framework to manage them appropriately. The CISO who does not embrace this foundational domain will be a CISO who will have a challenging time performing the essential task of a CISO—being the voice that helps the organization balance risk and reward so that the organization achieves maximum results while taking on the least possible risk to achieve those results. Getting risk management right is more than half the battle of a CISO.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.
hide01.ir

C|CISO

DOMAIN 2

Information Security Controls, Compliance and Audit Management

EC-Council

iacet.ir

Introduction

Ensuring an organization complies with applicable regulations and standards is a significant responsibility of a CISO. We are proving that an organization is compliant through auditing. Auditing guarantees the proper deployment of an information security (IS) program by a CISO. In this domain, we walk CISOs through the selection and management of IS controls to manage or mitigate risk identified through the risk process presented in Domain 1. An introduction to various control catalogs and frameworks will provide a baseline for CISOs to create their own IS control catalog. Applying those controls to comply with legal and regulatory standards and statutes is an art and science. This domain emphasizes understanding how to leverage the attributes of controls to ensure proper deployment.

Besides introducing CISOs to several of the most significant acts, laws, and regulations they would encounter, this domain covers significant distinctions and clarifications of their differences. This is important as CISOs will learn that a standard can be a regulation and be used to demonstrate compliance. In addition, the domain also covers how a CISO should function and interact, pre- and post-audit, to obtain an optimum result.

Knowledge Assumptions

This domain is based on assumptions that an information security (IS) practitioner participates in selecting and implementing various compensating controls to manage risk to information and assets and in reviews or audits of IS controls. A mature understanding of IS control behavior based on the attributes of controls is expected.

IS practitioners will be familiar with various legal and regulatory requirements applicable to their industry, company, and country, including identifying controls and safeguards that bring their organization into compliance with IS standards and practices. An expert understanding of one or more IS frameworks and a solid working knowledge of several information security standards, such as ISO 27001 and PCI DSS, are assumed.

The security practitioner can directly correlate the impact of IS controls on assets to achieve legal and regulatory compliance. It is assumed practitioners understand controls are managed according to a life cycle of continuous improvement involving selection, implementation, monitoring, and improvement.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. INFORMATION SECURITY CONTROLS

The foundation of an IS program is the controls used to protect information and assets from cyberattacks. Controls may be automated or manual processes, actions, or an apparatus that prevent, detect, or correct the effects of internal or external intrusions or attacks against an organization. They can range from established instructions to sophisticated cybersecurity products and services. CISOs must have robust controls to counter identified risks to their organization. Controls can have multiple uses, as many CISOs use controls equally to address governance, risk, and compliance.

Controls serving as safeguards of countermeasures are typically organized into various categories so that they may be deployed in sets to provide layers of defense to information and assets. Most controls fall under three main categories. *Manual* or administrative controls are policies or directives that instruct users of data and assets to behave in a manner that does not harm an organization. *Technical* controls are products or services that work in an automated fashion to protect information and assets. When manual or computerized controls are unsuitable for reducing risk to data and assets, compensating controls are used. *Compensating* controls are alternative safeguards used when business or technical constraints prevent an original control from being used. For example, if security patching cannot be performed, a server could be air-gapped or otherwise isolated from threat vectors that could introduce an exploit, which a patching control would have otherwise mitigated.

1.1. Identifying the Organization's Information Security Needs

As a CISO, you must identify your organization's information security needs. This is paramount before selecting the proper controls to protect your organization's information and assets. The first thing you should consider is the risk profile of your organization. Following the guidance in Domain 1, you will understand your organization's risk appetite and tolerance. These two factors influence your selection of the controls necessary to protect your organization's information and assets at risk. It would be best to be cautious in investing and applying security controls, as these measures should always align with the value of what is being protected.

hide01.ir

Your next objective will be establishing IS controls within your organization's business processes. This ensures that IS controls are naturally applied throughout the organization rather than considered after the fact. Establishing IS control measures will require that you work with business units and departments to learn their most critical business processes, which will help you identify where to invest your IS department's resources. The essential business operations need IS controls to ensure your organization can withstand cyberattacks.

1.1.1. Identifying the Optimum Information Security Framework

When reviewing cybersecurity frameworks and models, you will find this is like the adage "all roads lead to Rome." However, in this case, all roads lead to the National Institute of Standards and Technology (NIST) 800-53 or International Organization of Standards (ISO) and International Electrotechnical Commission (IEC) ISO/IEC 27001/27002. You will notice that many frameworks originate from either ISO or NIST, which is why many CISOs base their programs on either. Both frameworks are well documented and appropriately fit in designing an IS program.

HITRUST CSF®

The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) is a comprehensive cybersecurity and privacy framework initially intended for healthcare

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

organizations. HITRUST CSF has been the U.S. healthcare industry's most widely adopted security framework since 2010 (HITRUST, 2010). HITRUST CSF leverages the International Organization of Standards (ISO) and the International Electrotechnical Commission (IEC) standards 27001:2005 and 27002:2005. This design element alone makes it suitable for organizations outside of the healthcare field. One of the critical aspects of HITRUST CSF is that it has been cross mapped with widely used security standards that you may wish to include in your cybersecurity program.

The organization of HITRUST CSF includes 14 control categories, which contain 45 control objectives and 149 control specifications based on ISO/IEC 27001:2005 and 27002:2005. In addition to the ISO/IEC 27001:2005 and 27002:2005 baseline, HITRUST CSF includes three additional categories (domains): Information Security Management System (ISMS), Risk Management, and Privacy Practices. This framework is unique because each control comprises up to three implementation levels applied to healthcare organizations according to specific organizational, system, and regulatory factors [18].

Information Security Forum Framework

Founded in 1989, the UK-based Information Security Forum (ISF) is an independent, not-for-profit association of global organizations dedicated to investigating, clarifying, and resolving critical issues in cybersecurity. In 1998, ISF developed a compendium of information security good practices named the "Standard of Good Practice" (SoGP). It subsequently developed an assessment to identify benchmark environments and measure compliance with the SoGP. ISF revises SoGP biannually and adds new sections based on requests from ISF members and best practices research. The ISF's SoGP for Information Security (the Standard) is one of the most comprehensive information security frameworks available and provides complete coverage of the topics set out in ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework, CIS Top 20 Critical Security Controls for Effective Cyber Defense, and Payment Card Industry Data Security Standard (PCI DSS) version 3.1.

Although the framework is based on research by ISF and published in the United Kingdom, many organizations worldwide use it standalone or in conjunction with ISO or NIST.

The ISF SoGP framework focuses on controls in the following security domains:

- Audit and risk management
- Business continuity and availability
- Change management
- Operational monitoring
- Trusted Access

ISF has updated the context of its approach to cybersecurity through the release of its ISF Protection Process. This risk-based approach focuses on protecting the most critical information and assets. ISF begins with identifying critical assets and ends with watching the information life cycle.

ISF recommends using its Protection Process along with the broader protection capability of an organization. This capability consists of a range of different supporting elements as follows:

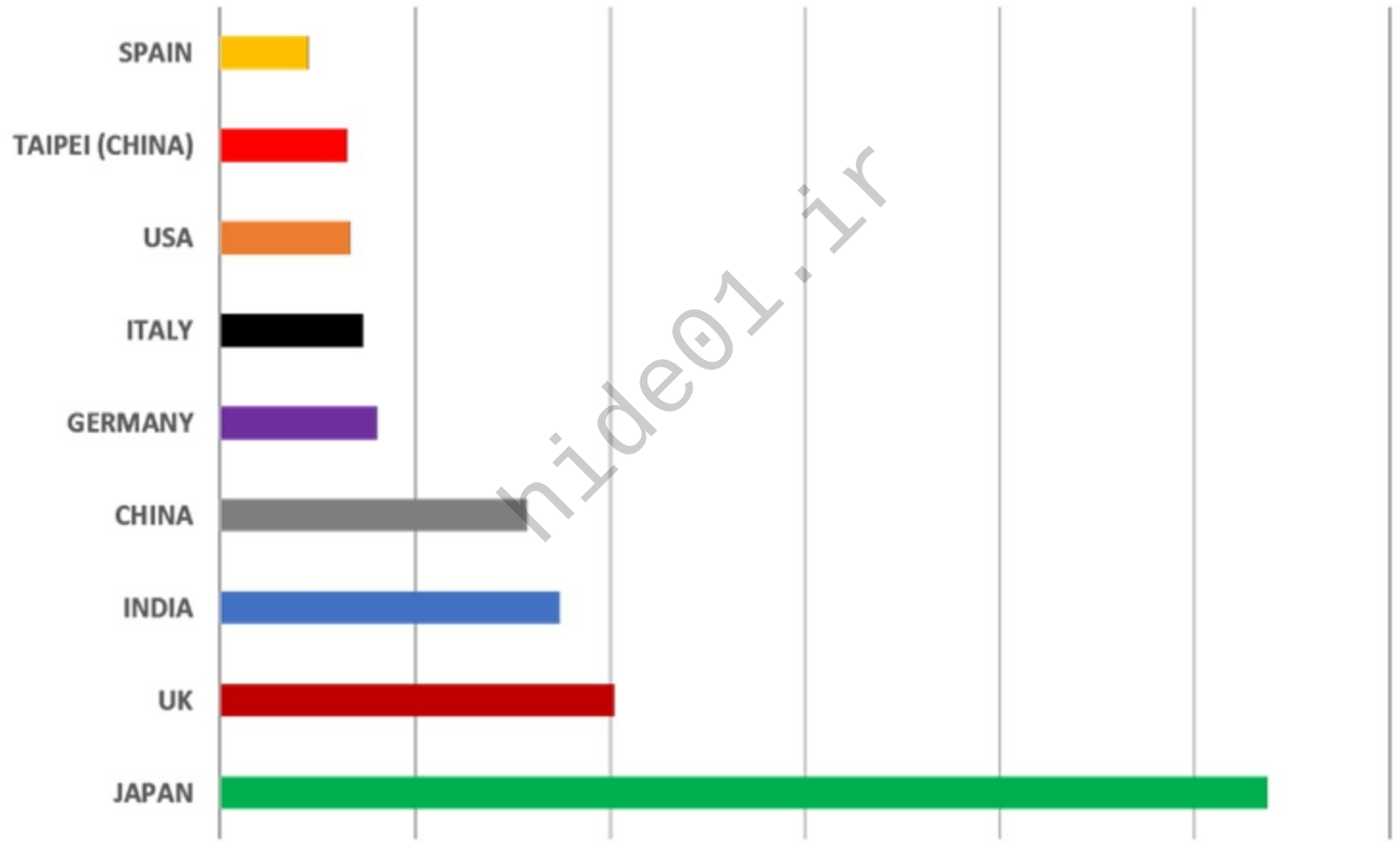
- Governance, risk management, and compliance (GRC): Set direction for security, promote ownership, and collaborate with stakeholders.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- People: Invest in skilled and experienced IT practitioners, security specialists, and risk experts.
- Technology: Automate protection of mission-critical information assets using security architecture, specialized technical security controls, and advanced security solutions.
- Security assurance: Determine policy, statutory, and contract obligations.

ISO/IEC 27001/27002 Information Security Management System (ISMS)

International Organization of Standards (ISO) and International Electrotechnical Commission (IEC) standards 27001:2013 and 27002:2013 are widely considered international information security standards. The ISO standard originates from 1995, known as the British Standard 7799, before it was adopted by ISO/IEC in 2000. Using the "all roads lead to Rome" analogy, consider ISO as Rome. ISO provides a link on its website to download an Excel file with ISO 27001 certification survey results. Between 2006 and 2016, over 33,000 ISO 27001:2005 certifications have been granted. Japan leads all countries with 26.85% of the certifications; the United Kingdom is second with 10.10%; and the United States ranks 12th with 3.3% [20]. Organizations are certified against the ISO 27001 standard, not ISO 27002.



hide01.ir

Figure 19: Top 10 27001 Certifications by Country

ISO 27001 and 27002 are complementary standards: ISO 27001 focuses on creating an information security management system (ISMS), and ISO 27002 provides a code of practice for information security controls. Many organizations base their programs on ISMS.

Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is a public framework that describes best practices in IT service management. It guides the requirements and measures that should be met and undertaken for the organizations to receive adequate IT services to support their business requirements. Information security is one of the defined ITIL services. A CISO can ensure an IS product or service is deployed correctly by implementing ITIL services. For example, capacity management, change/configuration management, continuity of operations, and so on should all be applied.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Because business alignment is a security goal, a CISO can leverage mature IT service delivery practices to provide information security services to the organization. ITIL's service operation (SO) processes are particularly helpful in supporting the security objectives by outlining best practices for delivering value regarding event management, identity management, problem management, and incident management processes [21].

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) originates from Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued February 12, 2013 (Executive Order, 2013). Within this order was the call for developing a cybersecurity framework. The CSF, published February 12, 2014, builds on and does not replace security standards such as NIST 800-53 or ISO 27001. It is a great starting point for organizations looking to improve their cybersecurity. NIST 800-53 is a regulatory document encompassing the processes and controls needed for a government-affiliated entity to comply with the Federal Information Processing Standards Publication 200—Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200) certification.

In contrast, the CSF is voluntary for organizations and allows more flexibility in its implementation. The fact that the framework is written initially for government agencies should differ from the reason not to use it. It covers information and assets irrespective of whether a bank or government agency owns them. NIST applies to any organization from any industry.

The CSF specifies that business drives an organization's cybersecurity activities and that cybersecurity risks should be part of an organization's risk management processes. CSF is comprised of three parts [22]:

- **Framework Core**: This part is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The core presents industry standards, guidelines, and practices that allow communication of cybersecurity activities and outcomes across the organization from the executive to the implementation/operations level. The framework core consists of five concurrent and continuous functions— identify, protect, detect, respond, and recover.
- **Framework Profile**: This part represents the outcomes based on an organization's business needs selected from the framework categories and subcategories. The profile concerns aligning standards, guidelines, and practices to the framework core in an implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "current" profile (the "as is" state) with a "target" profile (the "to be" state).
- **Framework Implementation Tiers**: This part provides context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's risk management practices exhibit the characteristics defined in the framework (e.g., risk and threat aware, repeatable, and adaptive). The tiers characterize an organization's practices from partial (tier 1) to adaptive (tier 4). These tiers progress from informal, reactive responses to agile and risk-informed approaches.

nide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

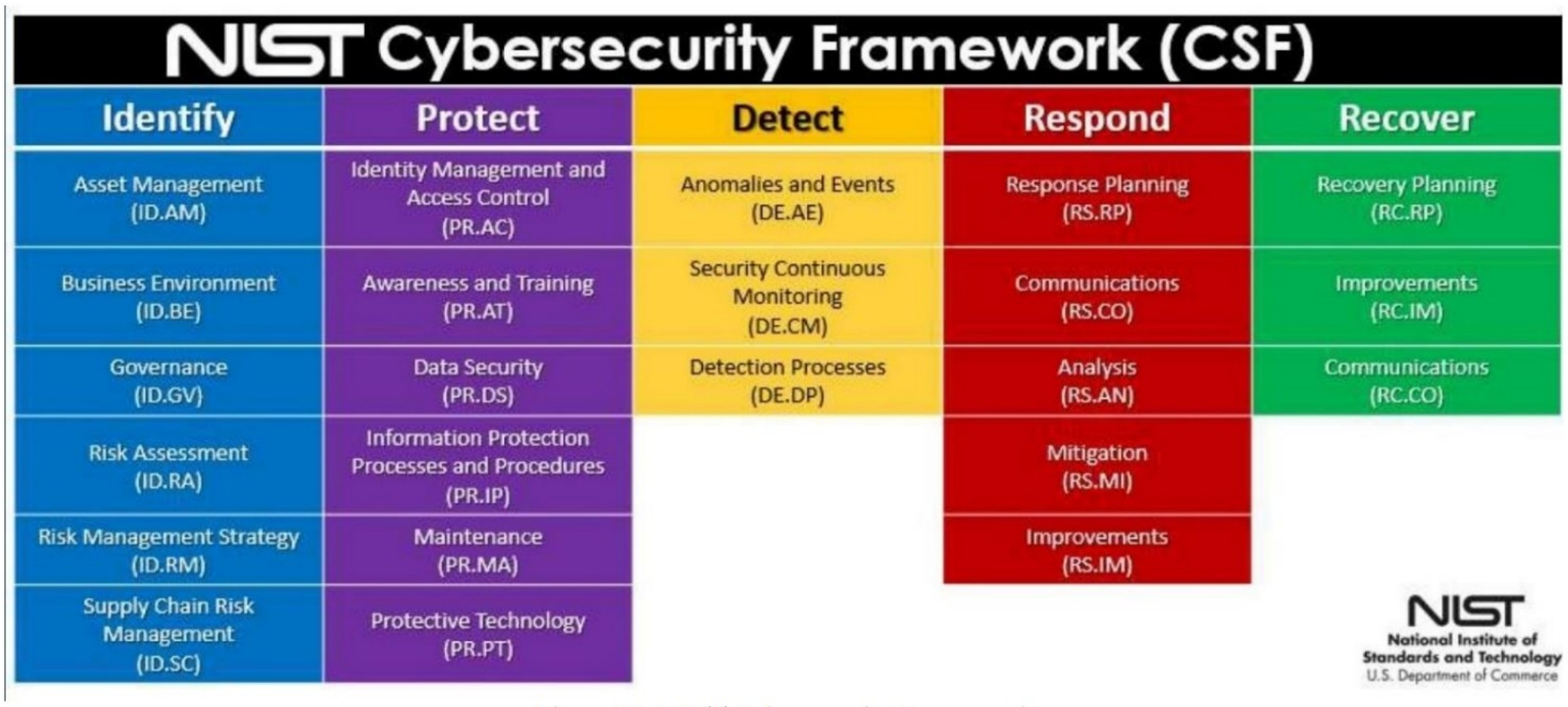


Figure 20: NIST Cybersecurity Framework

1.1.2. Designing Security Controls

Designing an IS control requires a balance between effectiveness and cost. The first level of controls requiring definition are vital controls. These controls are the ones that provide the optimum amount of protection singularly. By design, they detect, protect, or correct assets under attack. NIST defines this first layer as high-impact controls. ISO 27001 also lists their essential controls along with CIS' top 20. Designing a control requires fully accrediting it with attributes. Only through the assignment of these attributes can a CISO understand the behavior of a control. For example, is control oriented toward management, operations, or technical? Part of the design process also involves mapping controls to standards and regulations to leverage the duality of controls.

Control Attributes

As noted, the CISO must understand the types of controls available and the objectives of those controls. Each control used to mitigate risk or achieve compliance has three distinct attributes that the CISO must describe when making recommendations to business leaders:

- what the control is,
- what the control does, and
- how the control performs its objective.

Attributes facilitate the classification of controls. Two such features are manual and automated, distinguishing how the control is executed.

- **Manual Controls**—Manual controls require human intervention to perform the control. Examples include manually checking badges for authorized entry or manually reviewing audit logs. Manual controls are essential, but they are subject to human error. This can consist of forgetfulness, negligence, or misunderstanding requirements.
- **Automated Controls**— Automated controls apply logical intervention using technology to perform the control. Many logical controls exist as automated controls because they perform without human interaction. Computerized controls are preferred because of the accuracy, speed, and scalability with which they serve. They

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

are fallible. They require proper configuration and monitoring to provide maximum effectiveness.

Additional control attributes are covered in Section 2.1.5 "Control Classification."

1.1.3. Control Lifecycle Management

For controls to be continuously effective, they must evolve. Technology and organizations' legal and regulatory landscape are constantly changing, requiring controls to adapt to the environment into which they are deployed. Controls are assets to an information security program, and like any asset, they should be managed based on their lifecycle.

The following figure illustrates the lifecycle of an information security control:

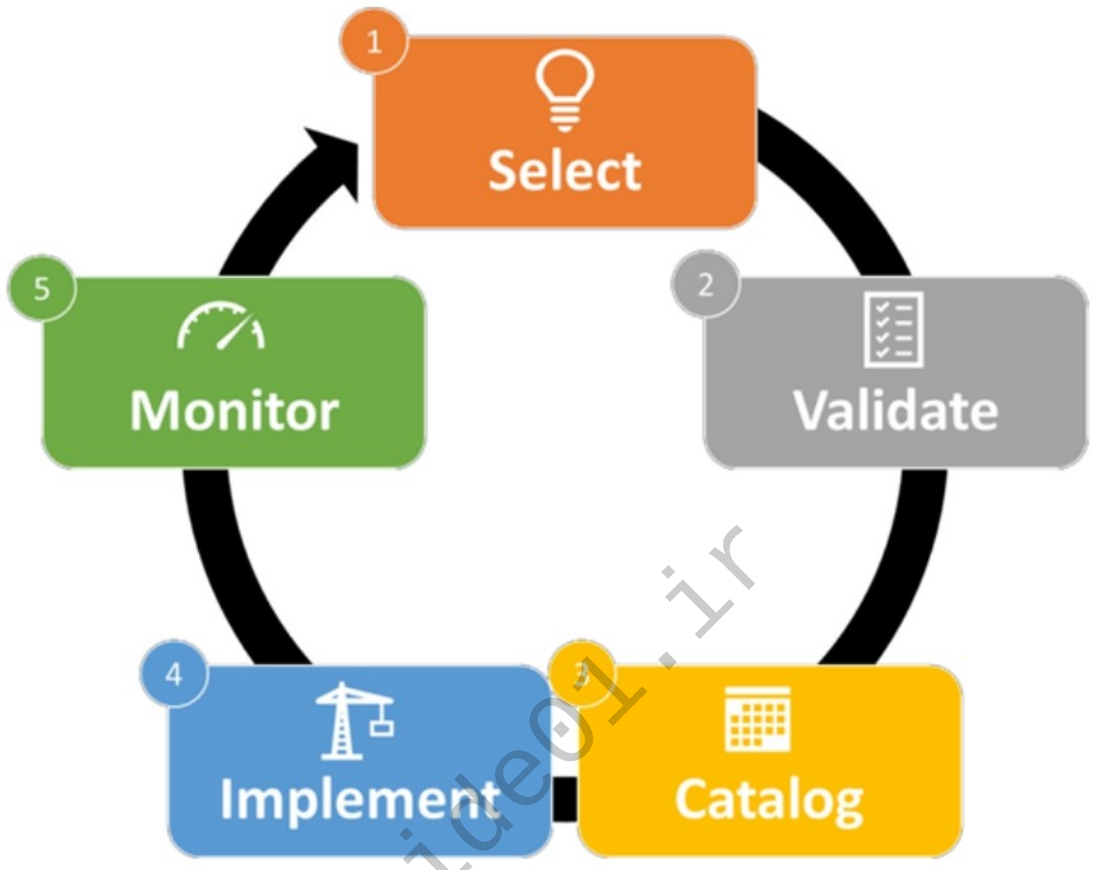


Figure 21: Control Lifecycle Management

- **Select**—The first phase of the lifecycle concerns selecting the proper controls based on their inherent attributes to manage or mitigate risk or comply with a legal or regulatory requirement. Thousands of published controls that are authoritative sources are available for CISOs to choose from. Controls can be found in all information security standards and several widely available control catalogs.
- **Validate**—The second phase of the lifecycle ensures controls are fit for purpose. To accomplish this, controls must be validated or evaluated depending on the type of control selected. For example, manual controls may be tested through user surveys, whereas technical controls may require proof of concept to ensure they protect information and assets according to design. The depth of control validation selected will depend on the level of confidence needed of the controls or that the controls exceed.
- **Catalog**—This lifecycle phase requires that controls be organized and inventoried in a catalog. A catalog can be a spreadsheet or a configuration management database (CMDB). In any case, the only proper way to manage controls is to enter them into a central repository where they can easily be identified and updated. Each control in the catalog can be determined by its type and all associated attributes, where it is deployed, and for what purpose. Logs simplify control reviews and audits as they provide

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

evidence of the control, its deployment, and which assets or information it protects.

- **Implement**—The fourth phase of the lifecycle involves implementing a control. Ways and means of implementing controls vary depending on the knowledge and experience of the control owner. A standard set of control parameters should be adopted to remove the ambiguity of how controls are deployed. These parameters should include an assigned owner, an associated policy the control enforces, a procedure describing the control's management, a process showing where the control is deployed, products or services that automate the control, and metrics that prove the control is functioning properly.
- **Monitor**—The last phase of the lifecycle involves metrics or some key performance indicator (KPI) showing the control is performing as intended. Deviations in the control's behavior baseline should be noted and remediated as part of the continuous improvement lifecycle. Controls can be monitored in several ways; however, an automated method should be used to reduce the time and effort of gathering and reporting KPIs.

1.1.4. Control Classification

Classifying controls allows a CISO to select the proper control for the right purpose. Several models have been introduced to help CISOs determine controls based on their assigned classification. Controls may be classified based on the purpose, as they may protect information and assets and comply with legal or regulatory requirements. For example, a "Backup Generator" disaster recovery control can be available as a corrective control. The attributes assigned to a control may help classify within the control catalog. Classifications also allow CISOs to produce records of controls for audits and reviews quickly.

hide01.ir

CIA Triad

The CIA Triad stands for Confidentiality, Integrity, and Availability. In 1994, The National Security Telecommunications and Information Systems Security Committee created the Comprehensive Model for Information Systems Security or the CIA Triad (reported within Principles of Information Security, 2009), widely used by CISOs worldwide. The model suggests three goals to protect information and assets:

- **Confidentiality**—Ensures that only an authorized person accesses data or an information system. User IDs and passwords, access control lists (ACLs), and policy-based security are some tools for achieving confidentiality.
- **Integrity**—Integrity assures that the data or information system can be trusted. Ensures that only authorized persons edit it and remain in its original state when at rest. Data encryption and hashing algorithms are vital processes in providing integrity.
- **Availability**—Data and information systems are available when required. Hardware maintenance, software patching/upgrading, data backup, and network failover ensure availability.

The following figure illustrates how the CIA Triad protects information and assets:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

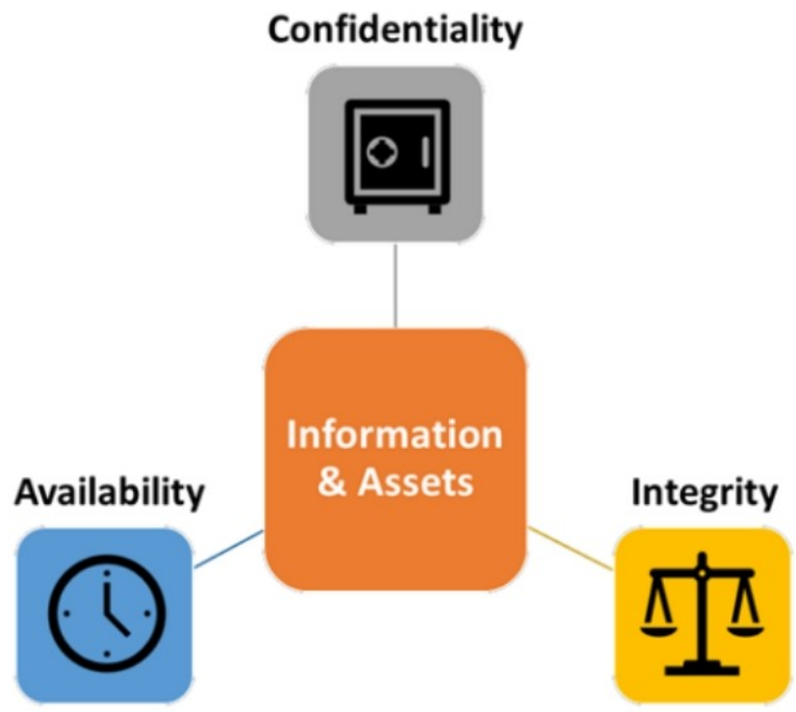


Figure 22: CIA Triad: CIA Triad

COSO PDC Defense-in-Depth Model

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [13] framework defines internal control as a process, effected by an entity's board of directors, management, and other personnel, designed to provide "reasonable assurance" regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

This figure illustrates how the PDC Model outlines a defense-in-depth approach to protecting information and assets:

hide01.ir

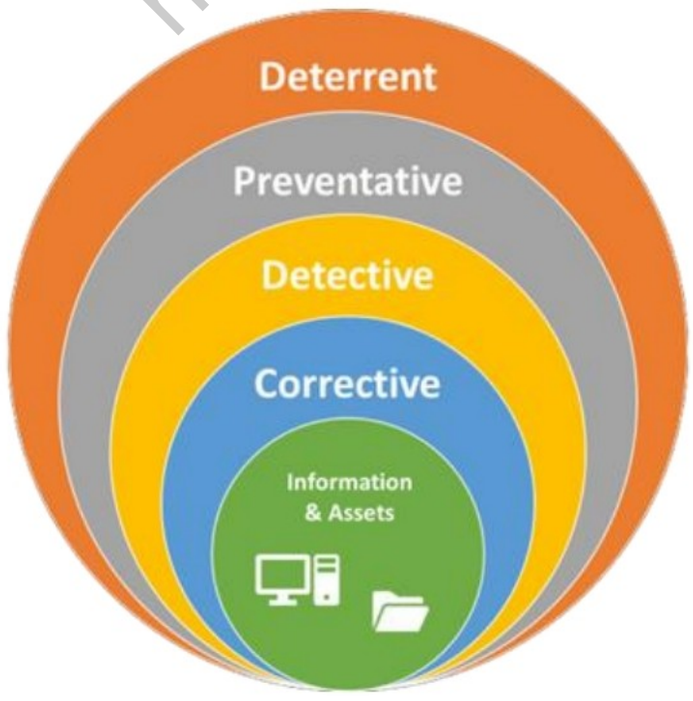


Figure 23: PDC Defense-in-Depth Model

- **Preventive Controls**—Prevention is the first line of defense in the control structure. Preventive controls protect the organization by preventing a threat from exploiting a vulnerability. This type of control proactively prevents a risk from being manifested.
- **Detective Controls**—Detective controls form the second line of defense. Detective controls identify the existence of strange or improper activity. Although detective controls identify potential threats, they do not prevent or address them. Solutions

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

designed to reveal unruly behavior for follow-up by security operations personnel involve detective controls. Detective controls are important, especially when preventive or corrective controls are challenging to implement. In addition, detective controls provide an important service in a layered defense approach because they can identify control failures in preventative and corrective controls.

- **Corrective Controls**—Corrective controls modify an environment and take action to restore the environment to its normal operating state. An intrusion detection system (IDS) is a detective control because it identifies improper activity. An intrusion prevention system (IPS) serves as a corrective control because it can terminate unauthorized sessions or take other actions to stop an attack and restore services.
- Over the years security practitioners added a fourth control to recognize the importance of controls that could deter a breach of security.
- **Deterrent Controls**—Deterrent controls discourage the exploitation of a vulnerability or system. For example, a warning banner that provides system-use notification is a deterrent to discourage unauthorized access to a system. This type of control does not prevent unauthorized access but helps deter it.

NIST Security Control Classes

The NIST information systems broad-based perspective. "As we push computers to "the edge," building an increasingly complex world of interconnected systems and devices, security and privacy continue to dominate the national dialogue. There is an urgent need to strengthen further the underlying systems, products, and services that we depend on in every sector of the critical infrastructure to ensure that those systems, products, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. NIST Special Publication 800-53, Revision 5, responds to this need by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations a comprehensive set of security and privacy safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud-based systems, mobile devices, Internet of Things (IoT) devices, weapons systems, space systems, communications systems, environmental control systems, supercomputers, and industrial control systems. Safeguarding measures include security and privacy controls to protect the critical and essential operations and assets of organizations and the privacy of individuals. The objective is to make the systems we depend on more penetration resistant to attacks, limit the damage from those attacks when they occur, and make the systems resilient, survivable, and protect individuals' privacy."

In 2001, NIST Special Publication (SP) 800-26, Guide for Information Security Program Assessments and System Reporting Form described three security control types: management, operational, and technical. NIST 800-26 was withdrawn in February 2005 when it was superseded by NIST SP 800-53. The NIST 800-53 special publication has been updated several times with its most recent release of NIST SP 800-53 Revision five. NIST 800-53 Revision four restructured the control classes of Administrative, Physical, and Technical controls to baselines that reflect the criticality of the system and the information protection requirements.

SP 800-53B contains security and privacy control baselines for federal information systems and organizations. It guides tailoring control baselines and developing overlays to support

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

stakeholders' and their organizations' security and privacy requirements. The Committee on National Security Systems (CNSS) Instruction 1253 provides control baselines and guidance for security categorization and security control selection for national security systems.

NIST SP 800-53 Rev. five is a collection of 1189 controls divided over 20 NIST control families that provide operational, technical, and managerial safeguards to ensure information systems' privacy, integrity, and security. Each family holds controls related to the specific topic of the family. Security and privacy controls may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms implemented by systems. Below is a table that lists the security and privacy control families and their associated family identifiers.

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Table 9: NIST Security Controls

NIST Minimum Security Controls

To assist organizations in selecting security controls for their information systems, NIST introduced the concept of baseline control [23]. Baseline controls are the starting point for the security control selection process. They are chosen based on the security category and estimated beneficial impact the control would have on protecting information and assets.

To accommodate various agencies' diverse needs and risk profiles, NIST SP 800-53 offers distinct security baselines, each mandating a specific number of controls. The low baseline, requiring 149 controls, caters to federal systems with minimal security needs, while the moderate baseline, which demands 287 controls, serves those with more substantial risk factors. Lastly, for the most critical and sensitive systems, the high baseline calls for the implementation of 370 controls, providing the most comprehensive level of protection.

- **High-Impact Baseline—**High-impact controls are usually used by financial services firms, healthcare organizations, and other organizations where the loss of confidentiality, integrity, or availability is assigned a Federal Information Processing Standards (FIPS) Publication 199 potential impact value of high. A failure could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals. They are typically deployed to protect sensitive information, personally identifiable information (PII), personal health information (PHI), cloud computing environments, and financial information.
- **Moderate Impact Baseline**—Moderate impact controls will account for many controls in an information security program. These controls are well suited for

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

situations where the loss of confidentiality, integrity, and availability is assigned a moderate FIPS Publication 199 potential impact value, and no security objective is set with a potential impact value of high. A loss would result in serious adverse effects on an organization's operations, assets, or individuals. Serious adverse effects could include significant operational damage to assets, monetary loss, or individual harm that is not loss of life or physical.

- **Low-Impact Baseline**—Low-impact controls are appropriate in situations where the loss of confidentiality, integrity, and availability are assigned a FIPS Publication 199 potential impact value of low. A loss would result in limited adverse effects on an organization. Correspondingly, security documentation is consolidated, and the number of security controls needing testing and verification is minimized.

1.1.5. Control Selection and Implementation

Organizations must consider the entire cost of controls they choose. These expenditures include acquisition, implementation, maintenance, operational support, and monitoring costs. An organization assesses these costs by evaluating the desired risk mitigation or compliance level and the asset's value to be protected.

The most common approach for selecting and implementing controls is following similar organizations' trends. An organization can limit the decision process by selecting best practices and recommendations from an industry or modeling controls as prescribed by peers or consultants familiar with the industry. Choosing controls based on industry or IT-wide trends and best practices is acceptable. Following trends set by others can be an effective method for selecting controls, except that the organization may expose itself to the same risks that others face.

The optimal approach to selecting and implementing controls requires spending time systematically understanding unique risks facing the organization. First, the organization performs an assessment. Then, it chooses the best mitigation strategy to address the identified threats while also considering organizational goals, risk tolerance, policies, and drivers influencing the risk management strategy.

- **Key Controls**—A key control originated in financial risk management, but the concept applies to information security. An essential control (high-impact baseline) is an indispensable control that mitigates significant organizational risk. If the control were to fail, no other control would prevent a threat from exploiting a critical environmental vulnerability. Failure of an essential control could be catastrophic if exploited.

- **Compensating Controls**—Compensating occurs when the recommended approach to implement a control is too expensive, impractical, or complex. The compensating control provides an alternative approach to achieve the intended outcome. Compensating controls can provide cheap alternatives for the original intent. When an organization selects a compensating control, the mitigation approach must meet or exceed the intended mitigation of the recommended (key) control.

1.1.6. Control Catalog

Control catalogs standardize their controls to identify the family or category of controls and each rule's objective and provide guidance or recommendations for implementing the control.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The two dominant catalogs of information security controls are ISO 27002 and NIST SP 800-53. Both catalogs give a comprehensive list of controls to address information security risks in an organization. The ISO catalog provides details for achieving the goals outlined in ISO 27001. In contrast, ISO 27002 offers significant detail to help an organization achieve the control selection process to meet risk mitigation goals and arrive at an acceptable level of residual risk. The NIST catalog provides a range of safeguards and countermeasures for organizations and information systems. These controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

The catalog selected depends on the needs of the organization. Within each catalog, a standardized approach is used to present each control. The catalog begins by organizing related controls into families or groups. The catalog identifies specific controls within each group with a reference number and a control title. Next, a control objective (a statement of what will be achieved) outlines the intended outcome or result of implementing the control. Control guidance then describes recommendations for achieving the intended outcome or result from implementing the rule.

NIST provides additional details and information on NIST SP 800-53. The section describing control enhancements offers guidance to extend the effectiveness of the base control. Controls selected to support risk management for an activity with a low-risk rating have enhancements defined to identify additional protections required at higher-risk ratings. The catalog also provides reference information to identify supplemental resources and other guidance to improve implementation or understanding of the control. The following table offers sources of control catalogs:

hide01.ir

Source	Title	Description
Center for Internet Security® (CIS)	CIS Controls™—v8	Catalog of 171 critical controls organized by 18 categories.
Cloud Security Alliance (CSA)	Cloud Controls Matrix (CCM)— v4	Catalog of 197 control objectives that are structured in 17 domains. Cross-mapped to 11 standards.
International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC)	ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection — Information security controls	Catalog of 93 information security controls organized into four themes.
National Institute of Standards and Technology (NIST)	NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations—R5 [23]	Catalog of 1189 essential controls organized into 20 control families.
Information Systems Audit	Cybersecurity Nexus™	Catalog of 72 controls

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and Control Association (ISACA)	(CSX)	organized by six categories.

Table 10: Control Catalog Sources Chart

1.1.7. Control Maturity

The maturity of an information security control can be evaluated according to the number of properties associated with the control that has been deployed. Properties include policies, metrics, products, and so on. The totality of maturity for all controls can provide valuable insight into the maturity of an entire IS program. A simple model can be used to help CISOs measure the maturity of IS controls. This model is referred to as the P6 Model. It is based on the premise that all controls require six properties to be deployed effectively.

The following questions can serve to identify the maturity of a control:

- **People**—Has an owner of the control been named, and are they professionally trained in how the control should function?
- **Policies**—Is the control required to enforce a specific policy?
- **Procedures**—Has the control been properly documented including all applicable attributes, and is it registered in a control catalog? Are standard operating procedures in place?
- **Processes**—Can the control be located within a closed-loop process showing where it engages in the organization's defense-in-depth strategy?
- **Products**—Is the control automated by scripts, technology, services, or other forms of automation?
- **Proof**—Are metrics and KPIs used to monitor the performance and effectiveness of the control and ensure transparent reporting?

h1de01.ir

You can weigh these properties by importance to arrive at a control maturity score that makes sense for your organization.

The following figure presents the P6 Model with sample weights assigned to each control property:

Figure 24: P6 Control Maturity Model (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-No Derivatives 4.0 International License)

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.1.8. Monitoring Security Controls

Once controls have been identified, categorized, and cataloged, they must be monitored. Monitoring can be accomplished through manual reviews or using an automated solution. Monitoring should include:

- **Review Date and Time—** Controls should be monitored by date and time and must be in the same time zone across the enterprise to coordinate events and trigger annual reviews.
- **Changes since Last Review—**Changes should be monitored to ensure they do not alter the original intent or design of the control.
- **Control Mapping Changes—**Controls should be monitored to verify they align with the intended initial standards and regulations. Additions of new standards and requirements should be noted for expanding the coverage of the noted controls.
- **Control Changes—** Updates to the standards controls should be monitored. Changes should be made accordingly.

1.1.9. Remediating Control Deficiencies

Suppose an audit or control review determines that controls are ineffective or do not exist. This information should be incorporated into the risk assessment process, and the organization should develop a mitigation plan. Inadequate and missing controls can expose an organization to more risk than expected because of the false sense of security when assuming adequate controls.

One option is to perform an abbreviated risk mitigation based on the original risk assessment to address findings in the audit. It might be possible to confine the level of rework to a risk treatment choice that meets the organization's goals. Remediation must occur once the organization accepts findings from the audit—and the findings are understood. An expected outcome is another data point to measure the effectiveness of remediation.

When performing remediation there are two ways to prioritize the program of work.

- Prioritize remediation according to potential risk impact.
- Prioritize remediation according to what can most easily be accomplished.

A few quick wins can help show progress and diligence in closing audit findings. However, addressing high-risk findings is critical because of the danger posed to the organization. Both options are viable, but the highest risk item should be the priority.

1.1.10. Maintaining Security Controls

Managing controls within its lifecycle requires the application of change management. Each time a control property or attribute is added, changed, or deleted, it should be tracked and documented by change control. Consider using version numbers for controls as well.

1.1.11. Reporting Controls

At least annually, control reports should be prepared and provided to the control owners to reemphasize the controls they are accountable for and have them verify the controls are still valid and up to date. The control catalog can be utilized for creating compliance reports. CISOs should have someone on staff to manage the control library or catalog to monitor and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

report on the state of IS controls.

1.1.12. Information Security Service Catalog

A service catalog is an organized repository of IS services available to the organization. Many CISOs have embraced this concept and begun to package IS controls and technology solutions as services. Services are priced for chargeback or as value added to departments or business units within the organization.

Table 11 presents a basic example of a service catalog entry:

Service Domain	**Service Family**	**Service Name**	
Enterprise Data Protection	Data Encryption	PKI	
Service Description	The PKI Administration service facilitates secure communications across and outside the enterprise. The service provides validation that the person (server) to which the organization is sending data to/receiving from is who they claim; it is a form of identity validation. This service is applied as needed to specific servers and devices. This service is closely related to and operates directly with the Certificate. Provisioning and Deployment Service.		
Standard Service Features	• Key exchanges • Key certificate • Key revocations • Key certifications • Key renewals.	Service Delivery Technology	Microsoft Public Key Infrastructure (PKI)
Delivery Channel	The PKI Service is the publication point for certificates and certificate revocation lists (CRLs) and Public Key policies within the Group Policy to control external CAs.		
NIST SP 800-53 Control Alignment	Protect (PR)	Access Control (PR.AC)	Key & Certificate Management
Version	1.0	**Date**	08.01.18
Service Owner	John Doe	**Service Architect**	Jane Doe
Service ID	ISEDP-02	**Delivery**	24 Hours
Service Cost	$2.35 per server	**Service Brochure**	www.PKI.com

Table 11: Information Security Service Catalog Example

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. COMPLIANCE MANAGEMENT

Compliance management concerns how an organization identifies legal and regulatory statutes it must adhere to and monitors and reports on the adherence to each applicable law, regulation, or standard. When properly implemented, compliance is embedded within business processes and operations, ensuring accountability. Instances of noncompliance are identified through reviews and audits and addressed through corrective action plans to regain compliance.

Before embarking on compliance management, knowing the definitions and differences between industry, legal, and regulatory terms is important. It is easy for a CISO to become confused with myriad legal jargon. As no standard or uniform body regulates information security, practitioners, vendors, and associations have defined a standard, regulation, framework, and so on. For example, ISO 27001 can be both a framework and a standard.

The following table provides an overview of the types and differences of compliance terms you will encounter as a CISO:

Term	Definition	Examples
Act	Provides detailed description explaining why and how laws are enforced as a formal decision. Enforceable by law.	The Health Insurance Portability and Accountability Act (HIPAA)
Executive Order	An official, legally binding mandate passed down from the president to federal agencies under the executive branch.	Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks
Framework	A general structure of something that represents a result or goal.	NIST Cybersecurity Framework (CSF)
Guideline	Recommended good or best practices created by consensus, which can be voluntarily followed.	Open Web Application Security Project (OWASP)
Law	Protects people, companies from unfair practices, and establishes the rules and regulations about specific situations.	State Breach Notification Laws
Presidential Policy Directive	A revocable presidential instruction leveraging presidential powers to compel government agencies to take a certain action.	Presidential Policy Directive 21 (PDD-21) – Critical Infrastructure Security and Reliance
Regulation	A specific rule or law prescribed to regulate conduct. Enforceable by law.	General Data Protection Regulation (GDPR)
Standard	A document established by consensus and approved by a recognized body that provides requirements and specifications.	Payment Card Industry Data Security Standard (PCI DSS)

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Statute	A Federal law, enacted by the U.S. Congress, must be followed by all states. Statutes preempt all other laws.	Computer Fraud and Abuse Act (CFAA)

Table 12: Legal Terms Definitions

A compliance management program has specific fundamental components, which, when followed thoroughly, ensure that the information security program meets or exceeds all applicable compliance requirements.

This figure presents a compliance reference model that may be used to define compliance efforts:

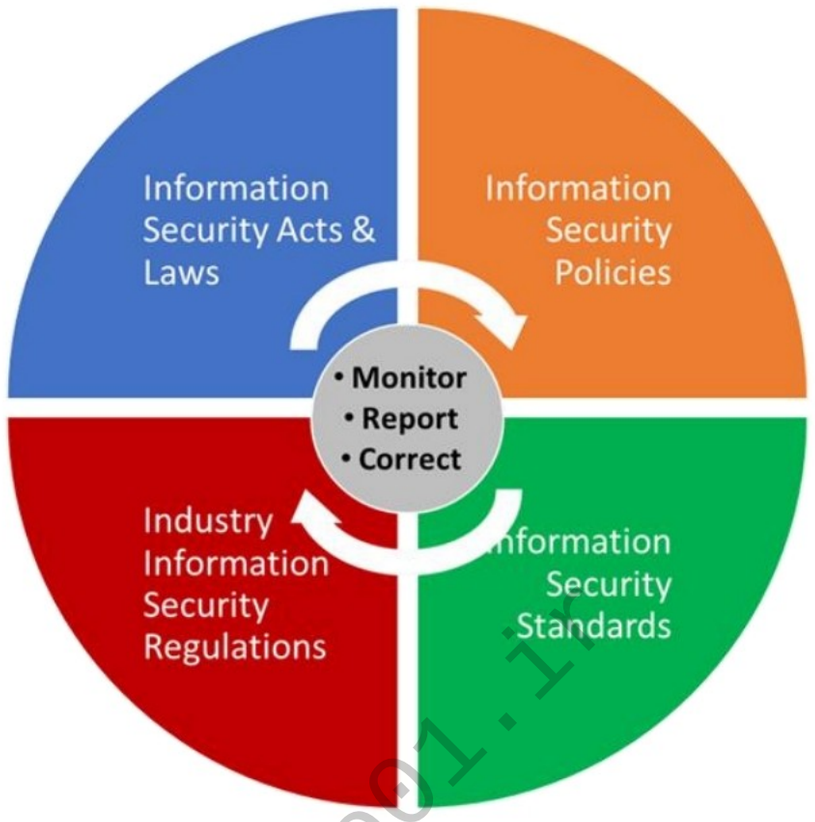


Figure 25: Compliance Management Reference Model

2.1. Acts, Laws, and Statutes

Statutes are written laws passed by a legislative body. Laws outline the principles and regulations established in a community by some authority that apply to its people, whether in the form of legislation or customs and policies recognized and enforced by a judicial decision. Organizations must comply with the requirements documented in the jurisdiction where a law was passed.

2.1.1. FISMA

The Federal Information Security Management Act (FISMA) [FISMA 2002], part of the E-Government Act (Public Law 107-347), was passed in December 2002. US FISMA 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other sources [24].

The Federal Information Security Modernization Act of 2014 (name change) amends the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 updated the cybersecurity practices defined in FISMA 2002 by codifying the Department of Homeland Security (DHS) authority to implement information security policies for nonnational security federal Executive Branch systems.

The FISMA of 2014 amends FISMA 2002 by providing several modifications that modernize federal security practices to address evolving security concerns. These changes result in less

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

overall reporting, strengthen the use of continuous monitoring in systems, and increase focus on the agencies for compliance and reporting that is more focused on the issues caused by security incidents. FISMA 2014 also required the Office of Management and Budget (OMB) to amend/revise OMB Circular A-130 to eliminate inefficient and wasteful reporting and reflect changes in law and advances in technology" [24].

Federal agencies, contractors, and other sources that use or operate a federal information system use the suite of NIST Risk Management standards and guidelines to develop and implement a risk-based approach to manage information security risk. As defined in FISMA 2002, "the terms 'Federal information system' means an information system used or operated by an executive agency, a contractor of an executive agency, or another organization on behalf of an executive agency." FISMA emphasizes the importance of risk management. Compliance with applicable laws, regulations, executive orders, directives, etc., is a byproduct of implementing a robust, risk-based information security program.

Important FISMA features:

- Periodic risk assessments
- Policies and procedures based on assessments.
- Quantitative risk rating—data-driven security model.
- Subordinate plans for information security for networks, facilities, and other sub-systems.
- Security awareness training for personnel.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls at least annually.
- A process to address deficiencies in information security policies (plan of action and milestones—POAM).
- Procedures for detecting, reporting, and responding to security incidents.
- Procedures and plans to ensure continuity of operations for information systems that support the organization's operations and assets.

2.1.2. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) improves the efficiency and effectiveness of the U.S. healthcare system by requiring national standards for electronic healthcare transactions and code sets, as well as unique health identifiers for providers, health insurance plans, and employers. The law includes Administrative Simplification provisions that require the U.S. Department of Health and Human Services (HHS) to adopt national standards for electronic healthcare transactions and code sets, unique health identifiers, and security [25].

Important HIPAA features:

- Electronic Transaction and Code Sets Standards: Requires the same healthcare transactions, code sets, and identifiers.
- Privacy Rule: Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Security Rule: Specifies administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.
- National Identifier Requirements: Requires that healthcare providers, health plans, and employers have standard national numbers that identify them on standard transactions.
- Enforcement Rule: Provides standards for enforcing all the Administration Simplification rules.

2.1.3. HITECH

The Health Information Technology for Economic and Clinical Health Act (HITECH) was created to promote health information technology adoption and meaningful use [26]. The law significantly modifies HIPAA by adding new requirements concerning privacy and security for patient health information. It also expands the scope of privacy and security protections available under HIPAA, increases the potential legal liability for noncompliance, and provides for more enforcement. Important HITECH features:

- Expansion of HIPAA security standards to "business associates" that perform activities involving the use or disclosure of individually identifiable health information
- Increased civil penalties for "willful neglect"
- Data-breach notification requirements for unauthorized uses and disclosures of "unsecured PHI"
- Stronger individual rights to access electronic medical records and restrict the disclosure of certain information
- New limitations on the sale of protected health information, as well as marketing and fundraising communications

r1de01.ir

2.2. Regulations

Regulations are rules or directives framed, maintained, and often enforced by an authority. They are the most authored by government entities.

2.2.1. GDPR

The General Data Protection Regulation (GDPR) (EU) 2016/679 [27] is a regulation in the European Union (EU) law on data protection and privacy for all individuals within the EU as well as the European Economic Area (EEA). GDPR governs the export of personal data outside the EU and EEA areas to achieve global compliance. The primary purpose of GDPR is to give citizens and residents back control of personal data. GDPR also addresses many of the deficiencies of the Data Protection Directive 95/46/EC that it replaces.

GDPR contains provisions and requirements for processing personally identifiable information (PII) of EU citizens and residents regardless of location. It also applies to companies with the EEA that process or handle PII. Key provisions of the GDPR include:

- PII must be built with data protection by design and by default.
- PII must be stored using pseudonymization or complete anonymization.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- PII must use the highest-possible privacy settings by default.
- PII cannot be made available publicly without explicit, informed consent of the citizen or resident.
- PII cannot be used to identify a subject without additional information stored separately.
- PII cannot be processed unless it is done under a lawful basis specified by the regulation.
- The data controller or processor of PII must receive unambiguous and individualized affirmation of consent from the citizens or residents to release information.
- Citizens and residents have the right to revoke their consent at any time.

GDPR further states that a processor of PII must disclose any data collection and declare the lawful basis and purpose for data processing, how long data is being retained, and if they are being shared with any third parties or outside of the EU. Data subjects have the right to request a portable copy of the data collected by a processor in a familiar format and to have their data erased under certain circumstances. Public authorities and businesses whose core activities center around regular or systematic processing of personal data must employ a data protection officer (DPO), who is responsible for ensuring compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

GDPR was adopted on April 14, 2016, and became enforceable beginning May 25, 2018; because the GDPR is a regulation, not a directive, it does not require national governments to pass any enabling legislation and is directly binding and applicable. With the United Kingdom scheduled to leave the EU in 2019, the UK granted royal assent to the Data Protection Act 2018 on May 23, 2018, which contains equivalent regulations and protections.

hiloo.ir

2.3. Standards

A standard is a measurement agreed upon by participants. A standard has less enforceability than a statute but often exists as a requirement. Many standards influence how an organization categorizes its business processes and conducts its affairs. Standards are typically formed by consensus.

2.3.1. ASD—Information Security Manual

The Australian Signals Directorate (ASD) [28] produces the *Australian Government Information Security* Manual (ISM). The manual is the standard that governs the security of government ICT systems. It complements the Protective Security Policy Framework.

The ISM comprises three documents targeting various levels of the organization, making the ISM accessible to more users, and promoting information security awareness across the government.

- 2016 ISM Executive Companion
- 2016 ISM Principles
- 2017 ISM Controls
- The *ASD Manual* is continually being revised, with the current version dated 2017. The 2017 version included the following updates:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Nine new controls (in Software Security, Secure Admin, and Cryptography).
- One hundred twenty-two controls have been updated.
- Changes to the cryptography controls represent a move to more robust encryption standards.
- The manual has been revised to improve the understanding and intent of many controls.

2.3.2. Basel III

Basel III [29] (or the Third Basel Accord or Basel Standards) is a global, voluntary regulatory framework on bank capital adequacy, stress testing, and market liquidity risk. Within Basel, concerns regarding operational and cyber risk convergence were raised. The Basel Committee on Banking Supervision members agreed to promote cyber risk management for financial institutions to determine bank capital requirements.

Risk management and Supervision, Basel requires financial institutions to assess their technical risk, establish controls, evaluate controls, and perform regular audits. Most organizations use ISO standards to achieve compliance with the Basel Accord. NIST can also be used to achieve compliance.

2.3.3. FFIEC

Federal Financial Institutions Examination Council (FFIEC) [30] has long audited financial institutions on their risk. DRP and BCM controls. FFIEC examiners use the *Information Technology Examination Handbook* (*IT Handbook*) as a guide to assess security risks to a financial institution's information systems. They evaluate the adequacy of the information security program's integration into overall risk management.

nilue01.ir

The FFIEC requires financial institutions to:

- Maintain effective information security programs commensurate with their operational complexities.
- Ensure strong board and senior management support.
- Promote integration of security activities and controls throughout the institution's business processes.
- Establish clear accountability for fulfilling security responsibilities.

In 2014, the FFIEC released the Cybersecurity Assessment Tool, which provides substantial information on cybersecurity controls to meet financial regulations. The FFIEC continually updates the tool, with the latest update occurring in May 2017.

2.3.4. ISO 27000 Family of Standards

One of the most used IS standards is published by the International Organization for Standardization (ISO). ISO publishes a family of standards covering a range of IS topics, including creating a security program, managing risk, and implementing an incident response plan. ISO standards are popular with organizations wanting to certify some or most programs.

The ISO family of standards includes over 30 standards. Below are the most used:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 26: Information Security-Related ISO Standards

ISO/IEC 27001:2013 | Information security management systems—Requirements [31]

This standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the organization's context. It also includes requirements for assessing and treating information security risks tailored to the organization's needs. The requirements in ISO/IEC 27001:2013 are generic and intended to apply to all organizations, regardless of type, size, or nature.

The standard includes ten clauses which cover:

- Scope of the standard
- How the document is referenced
- Reuse of the terms and definitions in ISO/IEC 27000
- Organizational context and stakeholders
- Information security leadership and high-level support for policy
- Planning an information security management system, risk assessment, risk treatment
- Supporting an information security management system
- Making an information security management system operational
- Reviewing the system's performance
- Corrective action

A full list of controls and their objectives are available to paying customers of the ISO.

ISO/IEC 27002:2022 | Information security, cybersecurity, and privacy protection — Information security controls [32]

This standard provides a reference set of generic information security controls, including implementation guidance and the selection, implementation, and management of controls, considering the organization's information security risk environment(s).

ISO/IEC 27002:2022 is designed to be used by organizations that intend to select controls in implementing an ISMS based on ISO/IEC 27001, implement commonly accepted information security controls, and develop their information security management guidelines.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27003:2017 | Information technology — Security techniques — Information security management systems — Guidance [33]

The guidance in this document focuses on the critical aspects needed for the successful design and implementation of an ISMS in accordance with ISO/IEC 27001:2013. It describes the ISMS specification and design process from inception to the production of implementation plans. It also describes the process of obtaining management approval to implement an ISMS, outlines a project to implement an ISMS, and guides how to plan the ISMS project – resulting in a final ISMS project implementation plan.

ISO/IEC 27004:2016 | Information technology — Security techniques — Information security management — Monitoring, measurement, analysis, and evaluation [34]

This standard provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of ISMS to fulfill the requirements of ISO/IEC 27001:2013, clause 9.1. It establishes:

- the monitoring and measurement of information security performance
- the monitoring and measurement of the effectiveness of an ISMS, including its processes and controls
- the analysis and evaluation of the results of monitoring and measurement.

Knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is essential for a complete understanding of this document.

ISO/IEC 27014:2020 | Information security, cybersecurity, and privacy protection — Governance of information security [35]

This standard provides guidance on concepts, objectives, and processes for the governance of information security, by which organizations can evaluate, direct, monitor, and communicate the information security-related processes within the organization. The document applies to all types and sizes of organizations.

ISO/IEC TR (Technical Report) 27016:2014 | Information technology — Security techniques — Information security management — Organizational economics [36]

This standard provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing resource requirements.

The standard applies to all types and sizes of organizations. It provides information to the top management to assist them in making information security decisions.

ISO/IEC 27017:2015 | Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services [37]

This standard provides guidelines for information security controls involved in providing and using cloud services, including:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002
- additional controls with implementation guidance that specifically relate to cloud services.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This recommendation provides controls and implementation guidance for cloud service providers and customers.

ISO/IEC 27018:2019 | Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [38]

This standard establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect PII under the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

The standard specifies guidelines based on ISO/IEC 27002, considering the regulatory requirements for the protection of PII, which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

ISO/IEC 27032:2023 | Cybersecurity — Guidelines for Internet security [39]

This standard provides:

- An explanation of the relationship between Internet security, web security, network security, and cybersecurity.
- An overview of Internet security.
- identification of interested parties and a description of their roles in Internet security.
- Critical Information Infrastructure Protection (CIIP).

This document is intended for organizations that use the Internet.

ISO/IEC 27034-1:2011 | Information technology — Security techniques — Application security — Part 1: Overview and concepts [40]

This standard provides guidance to assist organizations in integrating security into the processes used for managing their applications. It presents an overview of application security. It introduces definitions, concepts, principles, and processes involved in application security.

The standard applies to in-house developed applications, applications acquired from third parties, and where the development or operation of the application is outsourced.

ISO/IEC 27035-1:2023 | Information technology — Information security incident management — Part 1: Principles and process [41]

The standard presents basic concepts, principles, and processes with crucial information security incident management activities. These activities provide a structured approach to preparing for, detecting, reporting, assessing, responding to incidents, and applying lessons learned.

The guidance on the information security incident management process and its key activities in this document are generic and intended to apply to all organizations, regardless of type, size, or nature. Organizations can adjust the guidance according to their type, scope, and nature of business concerning the information security risk situation. This document also applies to external organizations providing information security incident management services.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27036-1:2021 | Cybersecurity — Supplier relationships — Part 1: Overview and concepts [42]

This standard is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts described in detail in other parts of ISO/IEC 27036. ISO/IEC 27036-1:2021 addresses the perspectives of both acquirers and suppliers.

ISO/IEC 27037:2012 | Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence [43]

This standard provides guidelines for specific activities in handling digital evidence: the identification, collection, acquisition, and preservation of potential digital evidence that can be of evidential value.

It guides individuals concerning everyday situations encountered throughout the digital evidence managing process. It assists organizations in their disciplinary procedures and facilitates the exchange of potential digital evidence between jurisdictions.

ISO/IEC 27037:2012 gives guidance for the following devices and circumstances:

- Digital storage media used in standard computers such as hard drives, floppy disks, optical and magnetic optical disks, data devices with similar functions
- Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards
- Mobile navigation systems
- Digital still and video cameras (including CCTV)
- A standard computer with network connections
- Networks based on TCP/IP and other digital protocols
- Devices with similar functions as above.

The above list of devices is an indicative list and not exhaustive.

2.3.5. NERC-CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) [44] plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

The NERC CIP compliance suite consists of 13 mandatory standards and over 100 requirements covering the security of electronic perimeters, the protection of critical cyber assets, personnel and training, security management, and disaster recovery planning.

CIP-002-5.1a	Cybersecurity — BES Cyber System Categorization
CIP-003-8	Cybersecurity — Security Management Controls
CIP-004-6/7	Cybersecurity — Personnel & Training
CIP-005-7	Cybersecurity — Electronic Security Perimeter(s)

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CIP-006-6	Cybersecurity — Physical Security of BES Cyber Systems
CIP-007-6	Cybersecurity — System Security Management
CIP-008-6	Cybersecurity — Incident Reporting and Response Planning
CIP-009-6	Cybersecurity — Recovery Plans for BES Cyber Systems
CIP-010-4	Cybersecurity — Configuration Change Management / Vulnerability Assessments
CIP-011-2/3	Cybersecurity — Information Protection
CIP-012-1	Cybersecurity – Communications between Control Centers
CIP-013-2	Cybersecurity – Supply Chain Risk Management
CIP-014-2/3	Physical Security (substations)

Table 13: List of NERC CIP Mandatory Standards

The CIP program coordinates all NERC's efforts to improve Bulk Electric System (BES) security. These efforts include standards development, compliance enforcement, risk and preparedness assessments, critical information dissemination, and increased awareness regarding crucial security issues. NERC's standards for governing critical infrastructure apply to entities that "materially impact" the reliability of the bulk power system. These entities include owners, operators, and users of any portion of the system.

Under NERC CIP, covered entities are required to identify critical assets and regularly perform a risk analysis. Policies for monitoring and changing the configuration of critical assets need to be defined, as do policies governing access to those assets. In addition, NERC CIP requires the use of firewalls to block vulnerable ports and the implementation of cyberattack monitoring tools. Organizations must also enforce physical and electronic controls protecting access to critical cyber assets. Systems for monitoring security events must be deployed, and organizations must have comprehensive contingency plans for cyberattacks, natural disasters, and other unplanned events.

Penalties for noncompliance with NERC CIP can include fines, sanctions, or other actions against covered entities up to $1 million/day/occurrence. Because NERC is a transnational organization, the penalties vary from country to country (including Canada and Mexico).

2.3.6. PCI DSS

The Payment Card Industry - Data Security Standard (PCI - DSS) [45] was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent security measures globally. PCI DSS provides a baseline of technical and operational requirements to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data (CHD) and sensitive authentication data (SAD).

PCI-DSS combines 12 requirements and corresponding testing procedures into six objectives:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Table 14: PCI DSS Security Requirements

2.3.7. NIST Special Publications

The U.S. National Institute of Standards and Technology (NIST) publishes standards, guidelines, recommendations, and research on computers, cyber, information security, and privacy. The 800 Special Publications series is the NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations, and reference materials.

The documents in the NIST Special Publications 800 series report on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. The series comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities.

hidoot.ir

SP 800 publications are developed to address and support the security and privacy needs of US Federal Government information and information systems or organizations managing data on behalf of the Federal Government. NIST develops SP 800-series publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 USC § 3551 et seq., Public Law (PL) 113-283. outline the requirements for US federal agencies.

A CISO from any organization may voluntarily adopt NIST's SP 800-series publications and has the flexibility to use these documents to help develop, support or enhance a security program. The documents provide foundational frameworks and are typically used to support security activities unrelated to the U.S. government. Moreover, they are widely used outside of government.

CISOs can find multiple benefits from implementing best practices from NIST. Using NIST guidelines, you can:

- Protect and issue sensitive data in accordance with regulations
- Protect critical infrastructure and information from insider threats, human error, and cybersecurity fatigue
- Aid in handling malware, evolving threat types and attack vectors
- Comply with other government regulations

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following presents several of the most commonly used NIST publications by CISOs:

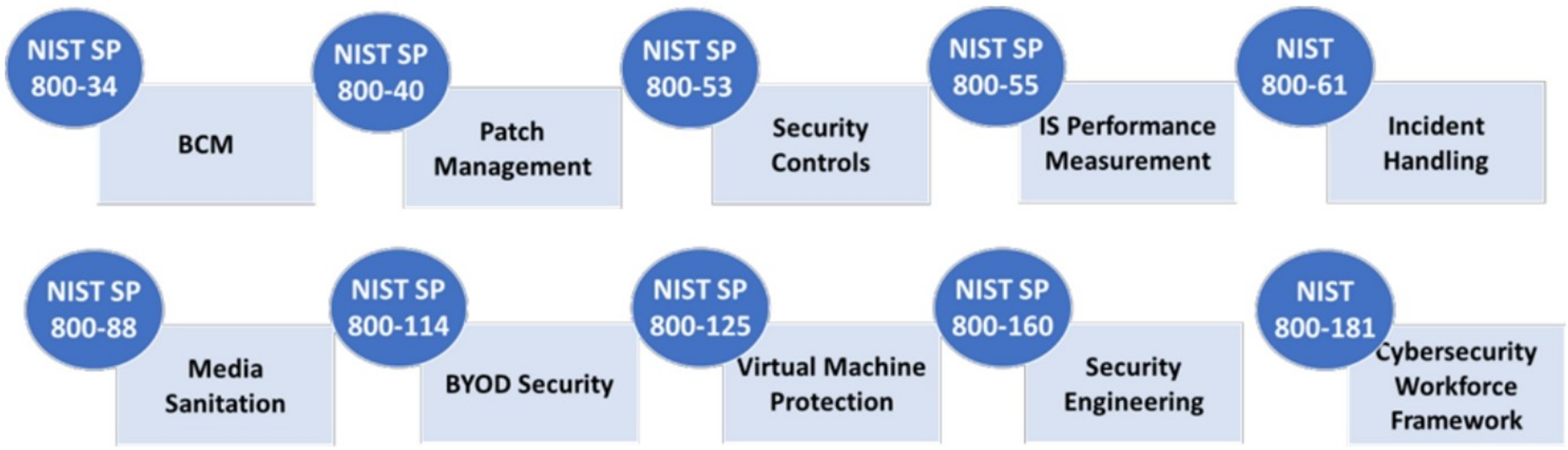


Figure 27: NIST Information Security-Related Special Publications

NIST SP 800-34 Rev. 1 / Contingency Planning Guide for Federal Information Systems [46]

Abstract: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. It also provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities.

NIST Special Publication 800-37 Revision 2 / Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy [7]

Abstract: This publication describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk, including information security categorization, control selection, implementation and assessment, system and common control authorizations, and continuous monitoring.

NIST Special Publication 800-39 /Managing Information Security Risk – Organization, Mission, and Information System View [8]

Abstract: The purpose of Special Publication 800-39 is to guide an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), corporate assets, individuals, other organizations, and the nation resulting from the process and use of federal information systems. Special Publication 800-39 provides a structured yet flexible approach for managing information security risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.

NIST 800-40 Rev. 3 / Guide to Enterprise Patch Management Technologies [47]

Abstract: Patch management is identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. It

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

provides an overview of enterprise patch management technologies and briefly discusses metrics for measuring the technologies' effectiveness.

NIST Special Publication 800-50 Rev. 1 / Building an Information Technology Security Awareness and Training Program [48]

Abstract: This publication guides federal agencies and organizations to develop and manage a lifecycle approach to building a cybersecurity and privacy learning program (hereafter called CPLP). The approach addresses the needs of large and small organizations and those building an entirely new program. The information leverages universally accepted standards, regulations, legislation, and best practices. The recommendations are customizable and may be implemented as part of an organization-wide process that manages awareness, training, and education programs for diverse employee audiences. The guidance also includes suggested metrics and evaluation methods to improve and update the program as needs evolve continuously.

NIST SP 800-53 Rev. 5 / Security and Privacy Controls for Information Systems and Organizations [49]

Abstract: This publication provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the nation from a diverse set of threats, including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

The publication describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions and business functions, technologies, environments of operation, and sector-specific applications. Finally, the consolidated catalog of controls addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms) and an assurance perspective (i.e., the measure of confidence in the security or privacy capability). Addressing functionality and assurance ensures that information technology products and the information systems that rely on those products are sufficiently trustworthy.

NIST SP 800-53A Rev. 4 /Assessing Security and Privacy Controls in Information Systems and Organizations [23]

Abstract: This publication provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within a practical risk management framework. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 5. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security and privacy control assessments that support organizational risk management processes and are aligned with the stated risk tolerance of the organization. Information on building effective security and privacy assessment plans is also provided with guidance on analyzing assessment results.

NIST SP 800-55 Rev. 1 / Performance Measurement Guide for Information Security [50]

Abstract: This document guides how an organization, using metrics, identifies the adequacy

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to justify security control investments adequately. The results of an effective metric program can provide valuable data for allocating information security resources and should simplify the preparation of performance-related reports.

NIST SP 800-61 Rev. 2 / Computer Security Incident Handling Guide [51]

Abstract: Computer security incident response has become critical to information technology (IT) programs. Because performing incident response effectively is complex, establishing a successful capability requires substantial planning and resources. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of hardware platforms, operating systems, protocols, or applications.

NIST SP 800-82 Rev. 3/ Guideline to Operational Technology (OT) Security [52]

Abstract: This document guides securing operational technology (OT) while addressing their unique performance, reliability, and safety requirements. OT encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change by monitoring and controlling devices, processes, and events.

NIST SP 800-88 Rev. 1 / Guidelines for Media Sanitization [53]

Abstract: Media sanitization is a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

NIST SP 800-114 Rev. 1 / User's Guide to Telework and Bring Your Own Device (BYOD) Security [54]

Abstract: Many people telework, using various devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. Each telework device is controlled by the organization, a third party (such as the organization's contractors, business partners, and vendors), or the teleworker, known as bring your own device (BYOD). This publication recommends securing BYOD devices used for teleworking and remote access and those directly attached to the enterprise's own networks.

NIST SP 800-125 / Guide to Security for Full Virtualization Technologies [55]

Abstract: SP 800-125 aims to discuss the security concerns associated with full virtualization technologies for server and desktop virtualization and to provide recommendations for addressing these concerns. Full virtualization technologies run one or more operating systems and their applications on top of virtual hardware. Full virtualization is used for operational efficiency, such as in cloud computing, and allows users to run applications for multiple operating systems on a single computer.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NIST SP 800-137A / Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment [56]

Abstract: This publication describes an approach for the development of Information Security Continuous Monitoring (ISCM) program assessments that can be used to evaluate ISCM programs within federal, state, and local governmental organizations and commercial enterprises.

NIST SP 800-160 Vol. 1 / Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [57]

Abstract: This publication addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, including the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems. It starts with and builds upon well-established international systems and software engineering standards published by the ISO, the IEC, and the Institute of Electrical and Electronics Engineers (IEEE). It infuses systems security engineering methods, practices, and techniques into the activities of systems and software engineering. The objective is to address security issues from a stakeholder protection needs, concerns, and requirements perspective and to use established engineering processes to ensure that such demands, concerns, and requirements are addressed with appropriate fidelity and rigor early and sustainably throughout the system's life cycle.

NIST SP 800-181 / National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [58]

Abstract: This publication describes the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), a reference structure representing cybersecurity work's interdisciplinary nature. It is a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen an organization's cybersecurity posture. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about identifying, recruiting, developing, and retaining cybersecurity talent. The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on various aspects of cybersecurity workforce development, planning, training, and education.

ninet1.ir

2.3.8. Statement on Standards for Attestation Engagements No. 16 (SSAE 16)

Statement on Standards for Attestation Engagements No. 16 (SSAE 16) [59] is an auditing standard for service organizations that replaced Statement on Auditing Standards No. 70 (SAS 70). SSAE became effective in 2011 and was developed by the American Institute of Certified Public Accountants (AICPA). SSAE 16 is a guideline and process to audit an organization's financial systems and controls. SSAE 16 is popular with organizations to show compliance with Sarbanes–Oxley's requirement (section 404).

SSAE 16 is a US standard closely aligned with the International Standard on Assurance Engagements (ISAE) 3402. Once an audit has been performed, two types of reports can be issued. The first one is a SOC 1 Type 1 report, an independent review of an organization's financial controls at a specific time. A SOC 1 Type 2 report is designed to provide the history (minimum six months) of how those controls have been managed and improved over time.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SSAE 16 guides an auditing method instead of mandating organizations follow a specific set of controls. This means that CISOs can continue to use ISO 27001/27002 and NIST Special Publications to prove their controls under SSAE 16.

3. GUIDELINES, GOOD AND BEST PRACTICES

Over the years, hundreds of papers and documents have been published on guidelines, good and best practices, and other advice on the seemingly optimum IS controls to deploy. Unfortunately, no central governing authority defines what is good or best practices industry wide. Many organizations refer to IS controls as best-in-class because they believe they must be the best. After all, several of their customers use them. It is almost impossible to gather a large enough sample size of organizations applying the same IS control to a similar IT platform to determine whether it is a best practice.

One common denominator for good and claimed best practices is that they are consensus-designed and vetted. As a CISO, it is highly recommended that only those IS controls be chosen that originate from organizations that rigorously define their controls from a broad membership that actively participates in working groups and subjects IS controls to peer review.

The following are two examples of consensus-based good practices:

3.1. CIS

The Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense is a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. The 18 *CIS Controls* are especially relevant because cyber experts update them based on actual attack data pulled from various public and private threat sources. [60]

hideol.ir

CSC 1	Inventory and Control of Enterprise Assets
CSC 2	Inventory of Control of Software Assets
CSC 3	Data Protection
CSC 4	Secure Configuration of Enterprise Assets and Software)
CSC 5	Account Management
CSC 6	Access Control Management
CSC 7	Continuous Vulnerability Management
CSC 8	Audit Log Management
CSC 9	Email and Web Browser Protections
CSC 10	Malware Defenses
CSC 11	Data Recovery
CSC 12	Network Infrastructure Management
CSC 13	Network Monitoring and Defense

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CSC 14	Security Awareness and Skills Training
CSC 15	Service Provider Management
CSC 16	Application Software Security
CSC 17	Incident Response Management
CSC 18	Penetration Testing

Table 15: CIS Critical Security Controls

3.2. OWASP

The Open Web Application Security Project (OWASP) Top Ten is a powerful awareness document for web application security that represents a broad consensus about the most critical web application security flaws [61]. It is also a powerful awareness document for web application security because of the information provided for each category: threat agents, attack vectors, security weaknesses, technical impacts, and business impacts. Each category in the OWASP Top Ten also helps organizations understand whether they are vulnerable to the concern. It also provides recommendations to prevent the attack, including example attack scenarios and potential mitigation steps.

The following figure lists the Top 10 concerns in 2017 and 2021:

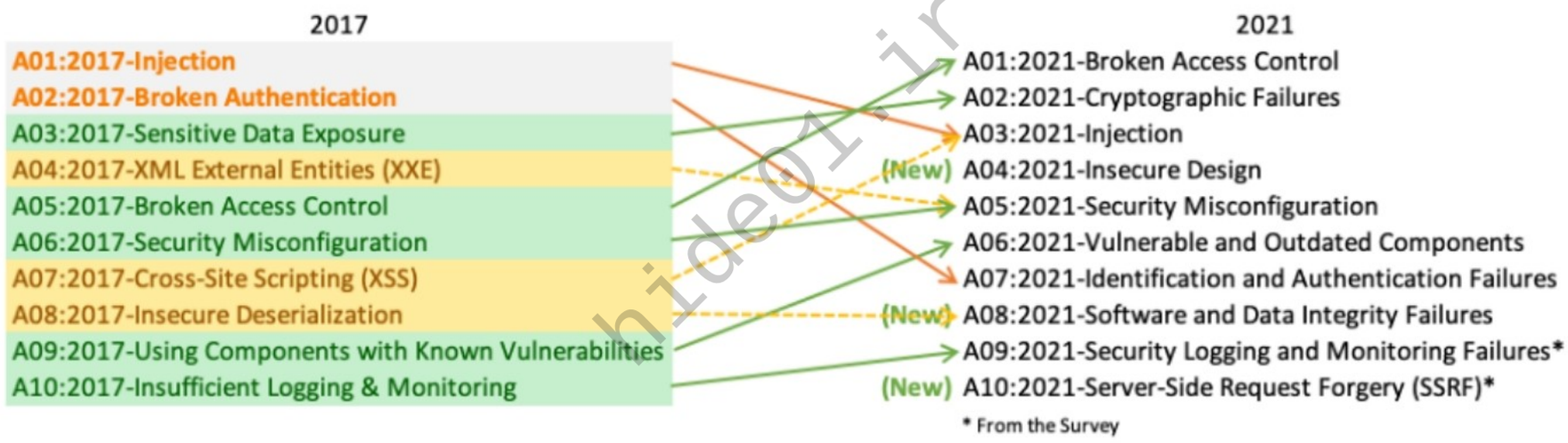


Figure 28: OWASP Top 10 Four-Year View

4. AUDIT MANAGEMENT

Audit management in this context is the process of CISOs overseeing their respective portion of internal and external audits. To effectively manage an audit, you must understand the audit process and the differences between internal and external audits, train your staff to interface with auditors properly, produce audit request documentation, and learn how to leverage existing software to support the audit process. As a CISO, a large amount of your time will be required to support audits of your department, especially considering the shift away from compliance-based to risk-based auditing.

An IS audit systematically evaluates the security of an organization's processes and systems, measuring how well they conform to established criteria or controls [8]. An IS audit aims to evaluate the effectiveness of controls used to mitigate risk in an organization or to measure alignment to a framework, internal compliance requirement, or regulatory requirement. Organizations invest considerable time and effort in building risk management and compliance programs. After applying controls to mitigate risks and ensure compliance, organizations must conduct internal audits to evaluate the effectiveness of those controls.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Audits sometimes occur as an independent assessment completed by a third party who evaluates effectiveness or confirms compliance. Otherwise, internal teams perform them to determine if controls are designed correctly, implemented according to their design, and whether the controls are operating to mitigate identified risks. An audit serves as a tool for continuous improvement of the information security program—the results of which can be used to recommend improvements.

4.1. Audit Expectations and Outcomes

What should you expect during an audit? Before providing that answer, remember that an audit is an information-gathering activity. The goal is *not* to identify new threats and vulnerabilities but to ensure that controls achieve their stated compliance and risk management objectives.

The outcome of an audit is helpful in many ways. Primarily, it helps determine if the organization is committed to complying with legal and regulatory requirements. Second, potential problems or shortfalls in implementing a risk management framework can be identified. Third, it can prove that controls applied to protect information and assets enforce IS policies and perform as designed [47].

4.2. IS Audit Practices

Performing an IS audit is different than the performance of a (classic) financial audit. On the one hand, financial audits are designed to validate to shareholders and investors that an organization is accurately reporting its financial health and that no accounting irregularities exist. Information Security audits are intended to confirm that information technology is safeguarded adequately to prevent compromises or interruptions from materially affecting an organization's finances and reputation or violating legal and regulatory requirements. So important is the performance of IS audits that several leading standards have published guidance on how IS audits should be planned and executed.

hidee1.ir

The more frequently referenced and followed IS audit practices are discussed in the following sections.

4.2.1. ISO/IEC Audit Guidance

ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection — Information security management systems — Requirements, clause 9.2 Internal audit [62]

This section of ISO 27001 defines the requirement to perform internal ISMS audits. This requirement reinforces the idea that the organization shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organization's requirements and the ISO 27001 standard and whether the ISMS is effectively implemented and maintained.

This section mentions several other essential concepts:

- Audits should consider the importance of auditing processes and areas and the outcome of previous audits. In other words, prioritize the audit activities and reassess processes that have previously required remediation.
- It is essential to define what is being audited and the boundaries of the audit. Audit criteria, scope, frequency, methods, and reporting shall be defined.
- Audits should be objective, and auditors should not evaluate their own work.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection — Information security management systems — Requirements, clause 9.3 Management review [62]

This section of ISO 27001 defines the requirement for top management to review the organization's information security management system at planned intervals to ensure its suitability, adequacy, and effectiveness. The objective is to improve the ISMS and to assist the CISO in deciding where to focus resources. Clause 9.3 also identifies specific inputs and outputs that help define the scope of the audit. This ensures that the management review and audit satisfy continual improvement requirements outlined within the standard.

ISO/IEC 27002:2022 | Information security, cybersecurity, and privacy protection — Information security controls, clause 8.34 Protection of information systems during audit testing [32]

The purpose of clause 8.34 is to minimize the impact of audits and other assurance activities on operational systems and business processes. The implementation guidance lists eight actions: audit planning, scope determination, and testing recommendations.

In addition to clause 8.34, many clauses and critical controls within ISO 27002 contain recommended audit or monitoring activities as part of the implementation guidance associated with controls. The following are some of the more essential references in the standard:

- **Independent review of information security (ISO/IEC 27002 control identifier: 5.35)**: Information Security An independent assessment will cover the organization's approach to managing information security and its implementation (including control objectives, controls, policies, processes, and procedures for information security). This should be done at planned intervals or after significant environmental changes.
- **Monitoring, review, and change management of supplier services (ISO/IEC 27002 control identifier: 5.22)**: Supplier services, reports, and records should be regularly monitored and reviewed. If available, audits of suppliers and sub-suppliers, in conjunction with a review of independent auditor's reports, should be performed against delivered services and products.
- **Review of user access rights (ISO/IEC 27002 control identifier: 5.18)**: Access rights to information and other associated assets should be provisioned, reviewed, modified, and removed per the organization's topic-specific policy and rules for access control.
- **Technical compliance review (ISO/IEC 27002 control identifier: 5.36 and 8.8):** Information systems should be regularly checked for compliance with security implementation standards.

ISO/IEC 27007:2020 | Information security, cybersecurity, and privacy protection — Guidelines for information security management systems auditing [63]

ISO/IEC 27007 provides guidance on managing an information security management system (ISMS) audit program, conducting audits, and the competence of ISMS auditors, in addition to the guidance contained in ISO 19011:2018 Guidelines for auditing management systems [[64]

ISO/IEC 27007 applies to those needing to understand or conduct internal or external audits

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of an ISMS or to manage an ISMS audit program.

ISO/IEC TS 27008:2019 | Information technology — Security techniques — Guidelines for the assessment of information security controls [65]

This standard, guides reviewing and assessing the implementation and operation of information system controls in compliance with an organization's established information security requirements, including technical compliance against assessment criteria based on the information security requirements established by the organization.

This document offers guidance on reviewing and assessing information security controls managed through an Information Security Management System specified by ISO/IEC 27001.

ISO/IEC TR 27008:2019 applies to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations conducting information security reviews and technical compliance checks. It is not intended for management system audits. Guidelines for auditing management systems have been described in the ISO 19011:2018.

NIST Audit Guidance

NIST SP 800-53 Rev. 5 | Security and Privacy Controls for Information Systems and Organizations—Audit and Accountability (AU) Family of Controls [49]

Within this publication are several controls included in the Audit and Accountability (AU) control family that focuses on the audit process. In addition to the controls from the AU family that guide an organization in building the capability for effective auditing into functions and systems.

- **AU-1 Policies and Procedures**—This control establishes policies and procedures for implementing selected security control and control enhancements.
- **AU-2 Event Logging**—This control enforces the standardization and collection of information system audit events.
- **AU-3 Content of Audit Records**—This control enforces a system's requirement to generate audit records with information that establishes the type of event when it occurred and other information supporting investigative processes.
- **AU-4 Audit Log Storage Capacity**—This control ensures organizations consider the type of audits conducted and the processing requirements when allocating audit storage capacity.
- **AU-5 Response to Audit Logging Process Failures**—This control ensures Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity.
- **AU-6 Audit Record Review, Analysis, and Reporting**—This control ensures the organization reviews and analyzes audit records for indications of inappropriate activity. It also guides reporting findings.

COBIT Audit Guidance

Audit and assessment success are at the core of the Monitor, Evaluate, and Assess (MEA) domain of COBIT five [66].

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section includes three distinct auditing processes:

- Performance and conformance
- The system of internal control
- Compliance with external requirements

Detailed techniques, guidance, and related goals and metrics are clearly defined for each process. When measuring the effectiveness of the audit process, the process goals and metrics are vital components of the analysis described in COBIT. Organizations using COBIT utilize process goals and metrics over a period to provide trending analysis. To do this, it is crucial to establish a baseline and **compare** progress against this baseline as the organization implements the audit process. If the metrics are not trending in the right direction, the audit program may be required to consider potential improvements.

4.2.2. Internal versus External Audits

As a CISO, you will encounter two types of audits where the information security program will come under the scrutiny of others, specifically the organization's internal auditing department and an external auditing firm retained by senior management to verify the financial and regulatory compliance of the organization. Some CISOs believe an internal audit is less formal than an external **audit**; however, both should be treated equally. Both parties perform types of audits independent of the information security department and report their findings to an audit committee. Internal and external audits review a range of risks to an organization, from supply chain, fraud, internal processes, and controls to the protection of information and assets. For the role of the CISO, this chapter focuses exclusively on auditing information security and continuity of operations controls included within the domains represented herein.

- **Internal Audit**: Typically, organizations will have an internal department staffed by employees utterly independent from other departments that report directly to an audit committee. Although primarily focused on financial controls, the internal audit group will have one or several employees with experience in information technology and security controls. The internal audit department's scope and depth of audits depend on the size of its audit staff. Compliance with legal and regulatory standards and statutes is a prime focus of many internal audit organizations today. Many organizations use internal audits to prepare for an external audit.
- **External Audit:** Public and private organizations alike retain public accounting firms that are independent companies with no financial or business interests in the organization other than the performance of an audit. Their focus is on verifying the financial statements and risk to the organization. External auditors perform annual statutory audits of an organization's financial well-being and operational integrity. They issue opinions on an organization's financial health and risk management. To support their views, they will evaluate internal controls to verify they manage or mitigate risk as designed or intended to prevent financial fraud, interference, or error. In some instances, an external auditing firm may perform a review where no test of controls is performed.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following summarizes the primary differences between internal and external audits:

Function	Internal Audit	External Audit
Independence	Internal department	External company
Reporting of Findings	Audit committee	Audit committee
Audit performance	Employees	Public accounting firm
Approach	Review controls	Test controls
Role	Consultant	Accountant
Focus	Risk management	Financial stability
Emphasis	Improve processes	Find faults and failures
Selection	Hired by organization	Shareholder vote
Allegiance	Management	Shareholders
Schedule	Ongoing process	Annually

Table 16: Internal vs. External Audit Function Comparison Chart

4.2.3. Partnering with the Audit Organization

As the CISO, you will be considered an auditee when an internal or external audit is performed in your department. You will hold this role from the announcement of an audit to the issuance of the audit **report** and remediation of findings. Cooperating professionally and openly with internal and external audit teams' requests is in your and the information security department's best interest. Senior management and the audit committee should create an environment to ensure the auditor–auditee relationship is non-adversarial. CISOs should foster a partnership of best practice sharing with internal or external auditors. However, there are some nuances with how you partner with an internal versus an external audit team.

Internal audit departments work as internal consultants and have a personal stake in identifying operational risk issues and engaging with you on potential solutions. You and the internal audit department aim to validate that information and assets are protected commensurate with their value. The internal audit department will engage with you to devise an annual audit plan, including the audit objectives, audit process, and the handling of audit findings. Discussions with internal auditing typically include impacts on your organization's risk posture and compliance relating to deficiencies found with your information security program. Internal audit departments can be instrumental in presenting issues to management where information security deficiencies result from limited funding or resources.

Collaborating with external auditors will be less collaborative than working with an internal auditing department. External auditors, by charter, maintain an arm's length distance from their auditees, preferring to find flaws in existing controls through independent testing and reporting control deficiencies to the audit committee. With that said, you can still build a partnership with an external auditing team through professional interactions and responses to their inquiries. Strive to create and develop a personal relationship with the external audit team. Although they may not share many best practices, they should provide many opportunities for

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

you to represent your side of a noted audit deficiency.

4.2.4. Audit Process

Internal or external audits follow a standardized audit methodology or process. Auditors recognize that an audit involves considerable time and resources and strive to operate efficiently and effectively following an organized approach. Once selected for an audit, you will receive formal notification, usually accompanied by a request for preliminary documents and a planning meeting. The audit commences with the arrival of the auditors in your department to conduct fieldwork gathering evidence. Once the fieldwork is completed, the auditors will draft their observations, work with you to correct any inaccuracies, and then issue a final report of findings. You can also expect to have auditors to follow your progress in remediating severe deficiencies. Audit processes may vary slightly, but the primary phases remain consistent:

- **Phase 1: Planning**: This phase is focused on creating the audit plan based on the documentation received from the auditee. The auditor will want to review previous audit reports to validate progress made in improving controls and existing proof that information security controls are performing as intended. CISOs can expect to have one or more pre-planning conversations with the auditors, including scheduling the audit activities. Auditors are willing to provide instructions on how deficiencies found during an audit would be noted and scored.
- **Phase 2**: **Fieldwork**: This phase is all about gathering evidence and proof that the information security program is performing in a manner that reduces risk to the organization's information and assets. External auditors will evaluate various controls and ask for concrete proof that various controls work sufficiently to help reduce risk. Internal auditors will primarily review control documentation and not perform testing. Auditors will also use an information security standard to validate if accepted controls are deployed.
- **Phase 3: Reporting**: This phase is focused on the compiling of evidence and analyzing the data to arrive at an opinion on whether the information security program is effective and suitable to protect the information and assets of the organization. The auditors may also come back with follow-up questions during their reporting phase. CISOs are customarily given a draft report to comment on and correct any factual inaccuracies that sometimes arise during fieldwork. They will also be asked to provide an action plan with timelines on when serious deficiencies noted will be corrected. The final audit report to senior management and the audit committee will be produced within this phase.
- **Phase 4**: **Follow-Up**: This phase occurs to validate if the organization has kept its commitments to remediate deficient controls within the estimated time limits. Auditors may request a progress report or require an onsite review of status depending on the seriousness of the noted deficiencies. For CISOs, this is a critical phase as you must provide proof deficiencies have been remediated, and if not, why?

hi_de91.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 29: Audit Process Flow

4.2.5. General Audit Standards

Audits are performed according to auditing standards, of which there are several widely followed international auditing standards. Standards define an audit's ethics, rigor, and integrity and the mandatory information assurance and security requirements. All audit standards contain the same basic principles of auditing concerning common audit language, evidence gathering, testing models, and reporting. Audit standards are primarily concerned with financial reporting; in support of that objective, all audit standards evaluate the security and continuity of an organization's financial systems. As the CISO of your organization, you should be familiar with the specific audit standards used by your internal and external auditors. Once identified, you will need to determine which information security control framework is referenced by your auditors.

The following table presents some primary auditing standards followed throughout the world:

Association	Acronym	Geography	Standard Name
American Institute of Certified Public Accountants	AICPA	United States	Statements of Auditing Standards
Confederation of Asian and Pacific Accountants	CAPA	Pan-Asia	Accounting Maturity Model

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Financial Reporting Council	FRC	United Kingdom	The International Standards on Auditing
Institut der Wirtschaftsprüfer in Deutschland e.V.	IDW	Germany	German Standards on Auditing
Institute of Internal Auditors	IIA	North America	International Standards for the Professional Practice of Internal Auditing
International Auditing and Assurance Standards Board	IAASB	International	International Standards of Auditing
International Federation of Accountants	IFAC	International	The International Standards on Auditing
The Japanese Institute of Certified Public Accountants	JICPA	Japan	Japanese Standards on Auditing
Public Company Accounting Oversight Board	PCAOB	United States	Auditing Standards
The Institute of Charted Accountants of India	ICAI	India	Indian Accounting Standards

Table 17: International Auditing Standards Chart

hide01.ir

Information Security Audit Standards

Discussed previously was the fact that general audit standards need to adequately provide for the deep level of guidance necessary to audit the information security controls of an organization. Auditors turn to audit standards written explicitly for information security to bridge this gap, such as COBIT® and COSO. This is not to say that COBIT® and

COSO are the only standards used or referenced by auditors. Many compliance management standards (e.g., ISO, NIST NERC-CIP) are referred to and used as audit standards. This is misleading, as they are not auditing standards. However, when coupled directly with a general auditing standard, they can be a referenced information security assurance framework.

To stay with the specific auditing context, only COBIT® and COSO will be discussed.

- **COBIT® 5: Framework for Information Technology Governance and Control**: The Control Objectives for Information and Related Technologies (COBIT) framework, advertised as an excellent practices-based framework, is available through the Information Systems Audit and Control Association (ISACA). ISACA, established in 1969, asserts in its literature and website that COBIT is the leading framework for governance and management of enterprise information technology (IT) with 115,000 constituents in 180 countries.

  Although not initially written for cybersecurity, many of COBIT's principles, enablers, and practices apply to building a cybersecurity program. COBIT released a professional guide in 2012 called COBIT 5 for Information Security to bridge the gap

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

in cybersecurity. In previous years, it offered the COBIT Security Baseline, security survival kits, and mapping to security standards such as ISO 27001. COBIT 5 for Information Security builds on the COBIT 5 framework to provide practical advice and guidance on implementing information security within an organization. This professional guide offers the same essential guidance as the COBIT 5 framework, with the main difference being its view through the lens of information security.

- **COSO 2013 Internal Control—Integrated Framework**: The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [13] is a joint initiative of five private sector organizations:
    - Institute of Management Accountants (IMA)
    - American Accounting Association (AAA)
    - American Institute of Certified Public Accountants (AICPA)
    - Institute of Internal Auditors (IIA)
    - Financial Executives International (FEI)

  Formed in 1985, COSO emerged to support the findings of the National Commission on Fraudulent Financial Reporting, also known as the Treadway Commission (IMA, 2017). The commission was established to create a standardized way to protect financial records through uniform controls. In 1992, COSO released a four-volume report entitled Internal Control—Integrated Framework. As a cybersecurity professional, you need to understand the concept of controls as a process originated from COSO. (The 1992 version was retired in 2014; the 2013 version is the most current release of the framework.)

  COSO has been widely adopted as a framework for internal controls; in 2015, the consulting firm Protiviti reported that 95% of U.S. Securities and Exchange Commission (SEC) filings they analyzed used some version of COSO as their control framework.

  Most companies use the 2013 COSO internal control framework, although many still use the 1992 version owing to its resiliency as a control framework.

4.2.6. Compliance-Based Audits

Compliance-based auditing (CBA) audits whether an organization complies with policies, regulations, standards, or legal statutes. Auditors would typically use a compliance checklist and interview the client to verify if they deployed the controls required for compliance. It has occupied audits for many years; however, it has lessened in importance as organizations and auditors find more relevance in risk-based auditing. Leading to this shift are the numerous accounts of organizations that were compliant with an industry security standard but were nonetheless successfully infiltrated by hackers. The wide adoption of governance, risk, and compliance (GRC) tools has automated CBA. An organization can efficiently and effectively produce compliance reports on any IS policy, regulation, standard, or law.

4.2.7. Risk-Based Audits

Information security organizations are often presented with a style of auditing referred to as risk based. Risk-based auditing (RBA) is an approach that focuses on the identification and analysis of risk in comparison to how an organization manages and mitigates that risk. This

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

approach dates to the late 1990s in the United Kingdom with the issuance of the Turnbull Report that set out a requirement for London Stock Exchange-listed companies to provide a statement to shareholders of the significant risks to the business. Subsequently, auditing associations adopted this approach to validate compliance with existing controls.

The basic premise of a risk-based audit approach is that auditors would first define the operations that, if compromised, would have the most significant impact on an organization. The areas of an organization with the most important potential impact would receive greater auditing attention. This approach results in more efficient and effective audits. This approach requires a strong understanding by the risk management auditors and proper calculations of business impacts. The cost of this approach to be performed by an external auditor has inhibited wider acceptance; however, internal auditing has found this to be quite effective in their domain as it links directly to an organization's overall risk management framework.

Risk-Based Internal Audit

Risk-based Internal Audit (RBIA) is a widely accepted practice by internal auditors. This auditing approach is focused on the inherent risk of the processes and activities of an organization and whether the proper information security controls have been applied to reduce risk aligned to an organization's risk appetite—this approach's core links to an organization's overall risk management framework. Domain 1 covers risk management, providing the tools for this precursor step to internal auditing.

In the simplest terms, the information security controls protecting the information and assets of your organization that would be impacted the most if compromised would be comprehensively audited to prove assurance. The audit process presented would change by inserting a Risk Profile phase ahead of the Planning Phase. Using GRC software, you can identify, define, and assess the risk of your auditable assets across the organization.

Figure 30: RBIA Phase

4.2.8. Managing and Protecting Audit Documentation

As the auditee of your department, you are entrusted with the production and safekeeping of the documentation you produce in support of an internal or external audit. Audits require lots of documentation; subsequently, you must establish an audit documentation repository for your department. The auditors will have their documentation repository; however, it is good practice for you to maintain your own protected copies. You must use version control and track what and to whom you provided audit support documentation.

The types of documentation that you should be prepared to provide upon auditor request include:

- Audit logs.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Control registries.
- Control assessments (previous).
- Information security policy manuals.
- Penetration test results.
- Process flows.
- Remediation action plans.
- Risk registries.
- Standard operating procedures.
- Most current vulnerability scan results [67].

Audit documentation can be subject to discovery in a data breach investigation, so it is in your organization's interest to establish client-attorney privilege for the most sensitive security assessment and audit information. Discuss with your legal counsel how best to establish attorney-client privilege.

4.2.9. Performing an Audit

As a CISO, you need to understand how audits are performed; this understanding will better prepare you and provide you with the how and why of the audit process. These steps represent the framework process used by internal and external auditors.

- **Step 1: Identify Areas Requiring Auditing—**Auditors will select areas of an organization they believe represent the highest risk, processes, or systems that have not been recently audited. They will also reference recent accounting or auditing guidelines for areas of particular interest based on an uptick in recent fraud or data breach cases. You should expect your department to always be on the audit list, although the scope will vary.
- **Step 2**: **Determine How Often Auditing Is Required**—Auditors will base the frequency of an audit on the level of criticality of an operation or process. In some cases, an audit is performed annually, in other cases, more frequently. For example, quality control is a form of audit and can occur daily.
- **Step 3**: **Establish an Audit Calendar**—Auditors have limited resources, requiring them to plan their audits as much as a year in advance. Scheduling audits on a business calendar ensures audits are done consistently.
- **Step 4**: **Notify Departments of Audit**—Auditors will notify departments of the time and scope of an audit once the audit calendar has been set. You will have a minimum of 30 to 45 days' advance notice.
- **Step 5**: **Prepare for the Audit**—Auditors prepare for each audit by understanding the audit area to conduct an efficient and effective audit with minimal impact on the auditee.

4.2.10. Evaluating Audit Results and Report

Audit findings provide feedback and opportunities for continuous improvement. They allow the identification and comparison of effective and ineffective controls. The results within an

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

audit report provide input for risk communication and remediation processes within an organization.

The structure and approach used to document the audit findings are essential. The report should begin with an executive summary defining the audit's scope and a concise summary of findings. The report should also contain a detailed summary of the controls audited, the methodology used to conduct the audit, findings, and evidence used to support the conclusions. The report will often document requirements and recommendations related to the audit results.

Audit findings are a roadmap for improving the organization. Once the organization agrees that the findings are valid, the information identified in the audit can help the organization prioritize additional improvements for the security program or the risk management strategy.

4.2.11. Remediating Audit Findings

Addressing audit findings is a fundamental part of cybersecurity program governance. Your program will be one of the most audited programs in your organization. You will need to respond to internal or external audit findings and recommendations. But precisely what are they? A finding is where an auditor notes a condition that is out of the normal boundaries of a standard. For example, a standard may state that you must have an encryption policy, and you do not. A recommendation is that you have one in place. Auditors also have degrees of findings ranging from serious infractions to simple recommendations. The auditor will also typically cite a specific standard clause, estimate the impact if you do not comply, and cite a cause for the deficiency. As a rule, you will have ten business days to respond, during which you can fully, partially, or not concur with the findings. In each case, you must provide a detailed response outlining your approach and time limit to remediate the audit deficiency. Addressing high-risk findings is critical because of the danger posed to the organization.

hide01.ir

Analysis and Interpretation of Audit Results

Audit findings provide feedback and opportunities for continuous improvement. They allow the identification and comparison of effective and ineffective controls. The results within an audit report provide input for risk communication and remediation processes within an organization.

Outcomes for Ineffective or Missing Controls

If the audit determines that controls are ineffective or do not exist, this information should be incorporated into the risk assessment process, and the organization should plan to perform treatment. Inadequate and missing controls can expose an organization to more risk than expected because of the false sense of security when assuming adequate controls.

One option is to perform an abbreviated risk treatment based on the original risk assessment to address findings in the audit. It might be possible to confine the level of rework to a risk treatment choice that meets the organization's goals. Remediation must occur once the organization accepts findings from the audit—and the findings are understood. An expected outcome is another data point to measure the effectiveness of remediation.

When performing remediation, there are two ways to prioritize the program of work.

- Prioritize remediation according to potential risk to the organization.
- Prioritize remediation according to what can most easily be accomplished.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A few quick wins can help show progress and diligence in closing audit findings. However, addressing high-risk findings is critical because of the danger posed to the organization. Both options are viable, but the highest-risk item should be the priority.

4.2.12. Leverage GRC Software to Support Audits

Governance, Risk, and Compliance (GRC) software can automate audit management, simplifying the process for auditors and auditees. GRC tools are beneficial when risk-based audits are performed, as risk assessments can be mapped to controls used to manage or mitigate inherent risk to specific assets. Within GRC tools, controls are mapped to legal and regulatory statutes, supporting your proof of compliance.

These tools can also catalog any issues raised during an audit. Audit issues can be prioritized, assigned to specific members of your information security organization, and aligned to action plans and exception reporting. Any audit work papers you produce and contribute can be managed in a workflow with resource and expense tracking assigned to support project management.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. SUMMARY

Domain 2 focused on how CISOs should create an effective IS controls catalog, how to achieve legal and regulatory compliance, and how to participate in an IS audit. However, the CISO must understand the risk profile of the organization as well as its critical business functions before applying IS controls. Regular audits are required to ensure these controls are fit for purpose.

CISOs today will find that a significant part of their day is devoted to compliance. The myriad state and country-level compliance statutes can be daunting and should be addressed with a formal approach to compliance management. A key challenge will be ensuring controls' duplicity to serve compliance and information and asset protection without doubling the effort and cost.

Auditing exists to evaluate control compliance and effectiveness. Auditing can apply to compliance when a requirement or standard is met. Auditing can also apply to effectiveness when a criterion, tool, or checklist confirms that a control, process, or approach effectively satisfies some objective. Both audit approaches leverage guidance that directs the process.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.
hide01.ir

C|CISO

DOMAIN 3

Security Program Management and Operations

EC-Council

Introduction

The Chief Information Security Officer (CISO) is a security program manager who directs activities to achieve an organization's information security and risk management goals. Domain 3 discusses security operations as one of the most essential information security programs a CISO will lead.

Content presented in Domain 3 assumes that the reader is familiar with standard project management concepts and vocabulary. This domain is not intended to prepare for project management certifications but to highlight important project management ideas that influence the delivery of products, services, and activities to support an organization's security objectives.

The discussion of projects does not map to a specific approach or methodology. Instead, it uses a top-down approach that identifies the information security portfolio as the highest management level. The portfolio contains significant efforts supporting the objectives of an organization. Within those efforts, the CISO manages and directs information security projects and activities to achieve the organization's information security and risk management goals. Domain 3 then evaluates security operations as a critical aspect of information security programs in an organization.

Knowledge Assumptions

The reader is assumed to have been involved in planning and executing information security–related programs and initiatives consisting of selecting staff, compiling basic budgets, and monitoring results. Involvement in the planning for the backup and recovery of some technology and various business functions is assumed.

Although the reader is not expected to be an expert in computer incident response, Domain 3 assumes that the reader has a basic understanding of the essential concepts and activities related to information security operations, such as event management, incident management, and digital forensic investigation.

The reader should also have experience identifying threats and vulnerabilities and understand the essential elements of penetration testing.

hideo1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. PROGRAM MANAGEMENT

1.1. Defining a Security Charter, Objectives, Requirements, Stakeholders, and Strategies

The CISO of the program will need to establish a dynamic and collaborative approach to managing the information security department. This involves developing a founding charter to shape the program's vision, defining clear objectives, outlining program requirements for efficient operations, identifying key stakeholders, and formulating practical strategies. This approach embraces openness and collaboration, aligning with the evolving landscape of information security practices.

1.1.1. Security Program Charter

Part of any solid program management effort is a program charter that defines the program to ensure its success. Too often, Information Security (IS) programs begin without a clear definition of success, and as a result, it becomes exceedingly difficult to measure success, let alone determine the program's effectiveness.

Organizations need to take the first step of creating a charter for the information assurance team to have a successful information assurance program. The benefit of these information security program charters is that they function like any other program charter. As a result, there is a solid body of knowledge governing what elements should exist in a mature program charter.

The following figure presents the elements a mature information security program charter should include:

hide01.ir

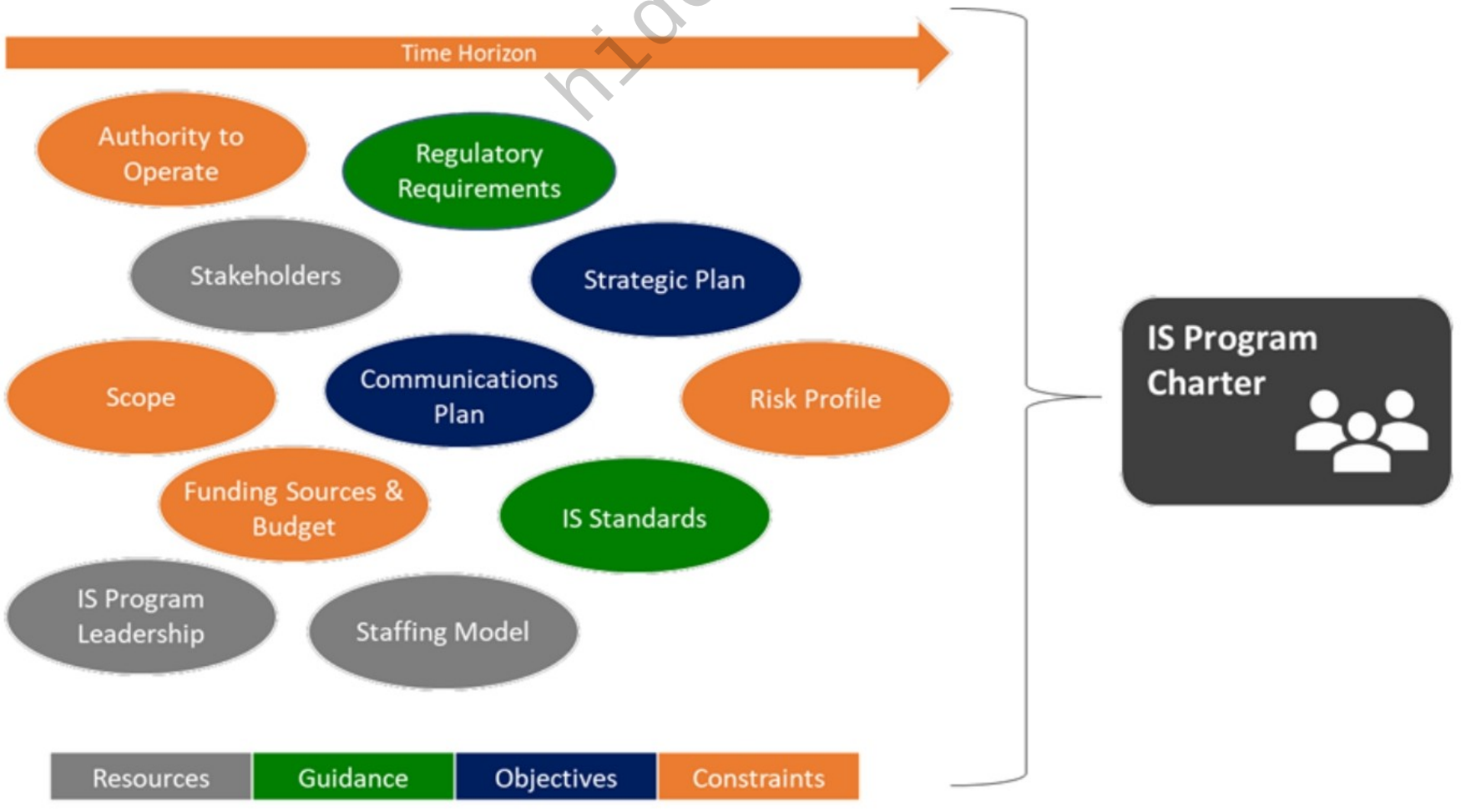


Figure 31: Information Security Program Charter Model

Each of the elements of the information security program charter is discussed next:

- **Resources:** Resources are the personnel who will support, staff, and lead the information security program.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Stakeholders: This refers to anyone with a personal stake in the program. This may include senior management, board members and employees Each plays a unique role, ranging from funding to authorization to operate.
- Program Leadership*:* The CISO formally names program leadership and their direct reports for each core component.
- Staffing Model: Organizations do not have unlimited budgets; therefore, an information security program must be scaled based on the budgeted headcount. Strategies for automation and staff augmentation can be used as a force multiplier.

- **Guidance:** This involves the external influences that guide the design of the information security program.
  - Regulatory Requirements: Understanding the regulatory requirements, the program must comply with ensures the program complies with legal and regulatory requirements.
  - Information Security Standards*:* The information security standards or framework that will be referenced will drive decisions in risk treatment and technology investment.
- **Objectives:** These involve planning documents that shape the foundation of the information security program.
  - Strategic Plan: The strategic plan is referenced to build the program.
  - Communications Plan: The program must have a communications plan of record to ensure transparency and knowledge transfer.
- **Constraints:** Information security programs comprise many sized projects, each with varying constraints. Boundaries that define the scope and authority of the programs can include the following:
  - Time Horizon: This is the period a program or project is authorized to operate. Information security programs continue indefinitely; however, some components may be time-bound.
  - Authority to Operate: This involves the statement of support from senior management granting authority for the information security program to exist and operate.
  - Scope: This involves identifying the organization, business units, functions, and external organizations the program has dominion over. The scope may also identify specific technologies.
  - Funding Sources and Budget: How the program will be funded is considered, identifying the funding sources and the allocated budget.
  - Risk Profile: Identifying the risk landscape, the program is designed to manage or mitigate is essential for properly allocating resources to protect information and assets.

  Incorporating recent Cyber-specific trends into the information security program charter is also essential. The following additional elements should be included:

mde01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cloud Strategy:** Outline the organization's approach to cloud security, including the adoption of cloud-native security solutions, the assessment of cloud service providers, and the management of cloud-related risks.
- **Artificial Intelligence (AI) and Machine Learning (ML) Integration:** Describe how artificial intelligence and machine learning technologies will be integrated into the information security program. This could include threat detection, anomaly detection, and pattern recognition powered by AI.
- **Cybersecurity Automation Framework:** Define the framework for automating routine security tasks and processes, such as vulnerability scanning, patch management, and incident response. Highlight the tools and technologies used for automation.
- **Data Protection and Privacy:** Emphasize protecting sensitive data and privacy considerations, especially in evolving regulations like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Specify data classification, encryption, and data lifecycle management strategies.
- **Threat Intelligence Integration:** Explain how threat intelligence feeds and sources will be leveraged to stay ahead of emerging threats and vulnerabilities. Describe how this information will be used to enhance security measures.
- **Security Awareness and Training:** Highlight the importance of ongoing security awareness and training programs for employees to ensure they are well informed about security best practices, especially in remote work and changing threat landscapes.

1.1.2. Security Program Objectives

An objective differs from a goal in that objectives are specific and easily measured, whereas goals are more visionary. Every information security program requires established and well-known objectives. An example of an objective would be reducing vulnerabilities by adopting approaches to assess, identify, prioritize, manage, and mitigate vulnerabilities.

The following are several examples of information security program objectives that may be referenced when developing program goals:

- Align the program with critical business functions by communicating operational risk.
- Build application security by integrating security planning within the Agile development methodology.
- Improve asset and information risk management by appointing business risk owners.
- Invest in protecting assets and information commensurate with loss values.
- Leverage human assets as the first line of defense through practical security awareness training.
- Recover critical business functions with minimal impact on customers.

1.1.3. Security Program Requirements

Before creating a security program, its design requirements must be appropriately identified and cataloged. Finding out later that a design element needed to be included could prove costly. The following checklist may be used as a guide in gathering the program's minimum

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

design requirements:

Identify the Information Requiring Protection: Here, a thorough understanding of the information processed by the organization is required. Preferably, this will include a data classification schema that presents the various data types and their associated levels of criticality.

Inventory Legal and Regulatory Requirements: The controls deployed to protect information and assets will be influenced by the types of legal statutes, industry regulations, and security standards the organization must comply with. This requires an inventory and analysis of all relevant legal and regulatory requirements.

Define the Attack Surface: Knowing the hardware, software, and networking components is essential for determining the security technology required to protect these assets. An asset inventory will guide such things as security technology licensing, logging storage requirements, firewall throughout, and many other security technologies decisions.

Determine Risk Profile: Information security programs are designed to manage and mitigate organizational risk. Understanding the risk to the organization allows the CISO to apply security controls where most needed to protect the most critical assets and information.

Business Impact Assessment (BIA): A BIA determines the value of information and assets if impacted by a breach of security or data loss event. Knowing the value of assets drives the application of security controls where the measures to protect the investment are commensurate with its value.

1.1.4. Security Program Stakeholders

A stakeholder is any person interested in a program or project. Stakeholder input for planning, a component of stakeholder expectation management, helps ensure that information security programs communicate effectively to manage expectations and deliver expected outcomes.

Stakeholder expectation management centers around building, monitoring, and nurturing positive relationships with stakeholders while effectively managing their expectations. This begins with the establishment of a well-structured communication strategy. Organizations must adapt and refine these strategies to align with the distinct needs of various stakeholder groups. To facilitate this process, a template is presented in the following table for identifying individual stakeholders, selecting appropriate communication methods, understanding their fundamental interests, specifying their preferred roles within the program, and determining the frequency at which updates, and information should be shared. It is important to delve into specific strategies for engaging stakeholders, including executive stakeholders, technical experts, and end users. The CISO should embrace the utilization of diverse communication channels such as email, face-to-face meetings, and video conferencing.

The plan only requires a few details. Each information security program should document each stakeholder's identity, requirements, and expectations to increase the opportunity for successful delivery as part of program execution.

The following is a stakeholder management plan that is recommended for each key stakeholder of the security program:

ITDOO1.IR

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Stakeholder Management Plan	
Stakeholder Name	Jane Doe
Program Interests	(Enterprise Resource Planning) ERP and System, Applications, and Products (SAP) application development
Program Role	Application Development Manager
Success Goals	Integration of security protocols within Agile development sprints
Communications and Reporting Strategy	Weekly Appel status meeting attendance Monthly application security incident reports
Communications and Reporting Schedule	Monthly

Table 18: Sample Stakeholder Management Plan

1.1.5. Security Program Strategy Development

Developing a strategic plan is a journey rather than a destination. Strategic plans are meant to be continuously reviewed and updated to reflect changes in business direction and technologies. CISOs need to understand the business context of their Information Security (IS) program and continually check in to ensure the program remains aligned. Strategic plans work best based on a solid mission, vision, and values to communicate the program's worth. Organizational principles set the tone of how the program will operate. Goals and objectives specify what you want to accomplish and how you achieve those goals and objectives through the application of strategic actions.

hide01.ir

Figure 32: Strategic Plan Development Life Cycle

The following are the four basic approaches to developing a strategic plan:

- **Protect the Crown Jewels Approach:** A traditional strategy follows the medieval concept of safeguarding valuable treasures like crown jewels. In this approach, the most critical assets and information are placed in the middle, with layers of defense encircling them. These defensive layers include dealing with challenges like boundary

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

issues and implementing Bring Your Own Device (BYOD), which can make this approach quite complex.

- **Risk-Centric Approach:** In contrast to the traditional 'Protect the Crown Jewels' model, the risk-centric approach prioritizes identifying and mitigating risks based on their likelihood and potential impact on the organization. This approach recognizes that not all assets are equally critical and focuses resources on protecting those most vulnerable or with the most significant potential for harm. It strongly emphasizes continuous risk assessment, adaptive security measures, and the flexibility to adjust security controls based on evolving threats and technology trends. The risk-centric approach is better suited to the dynamic and decentralized nature of modern IT environments, including cloud computing and BYOD, where the focus is on managing risk rather than merely safeguarding specific assets.
- **Football Playbook Approach:** An approach preferred by organizations with substantial resources and funding is the sporting team approach to executing an information security program based on a published playbook. Here, every situation has a preprogrammed play to repel attackers. Playbooks are continually evolving through a process of attack testing and simulations. Using red, blue, and purple teams, information security organizations evaluate attack scenarios to develop plans to counteract attacks.
- **Attack Surface Approach:** This approach is based on limiting and defending against threat vectors that could be used to launch an attack. Here, the entire enterprise is viewed as something that could be attacked. Strategies focus on threat identification and vulnerability reduction.

1.2. Executing an Information Security Program

Executing the information security program initiates the collection of processes and activities constructed in the program's design phase. The organization implements the security program in the execution phase.

Program execution focuses on measuring outcomes against objectives. Measuring outcomes is important because this activity ensures that the program achieves the intended goal. An example would be measuring the activities of event identification and remediation. Programs that do not complete the intended purpose can be adjusted to improve performance. Successful programs typically use standards and procedures, such as the capability maturity model integration (CMMI), to improve maturity.

1.3. Defining and Developing, Managing and Monitoring the Information Security Program

Much of the financial management conducted by the CISO falls within management accounting, which focuses on information used within the organization to help internal decision-makers plan, direct, and control business operations.

To ensure you have an equal footing with peer managers within your organization, a quick tutorial on financial management and accounting is provided as follows:

- **Assets:** The CISO should understand the foundational concept of assets and liabilities because of the perspective they influence within the organization, especially for the

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information security program.

Assets are items of value the organization owns. The CISO has stewardship over many assets required to support information security programs and activities. For example, security assets include third-party contracts, security appliances, software, and tools. These assets are important because the CISO must provide effective management of them. This would consist of ensuring funding is available to replace assets that have exhausted their useful life (or to procure new assets).

- **Cost Benefit Analysis (CBA):** It provides the most straightforward calculation among financial comparison tools but is also the least precise. This model is often used to produce quick mental comparisons of two options. The outcome of a CBA comparison will help determine whether a project is financially feasible or another project should be pursued. CBA analyzes decisions by identifying the benefits of a decision in terms of total value and subtracting the costs associated with taking that action.

Unfortunately, calculations used to estimate the total benefit or value of an intangible asset or activity are difficult. Models that apply a monetary value to the concern are often required to support this analysis. The organization must agree on the valuation model selected to provide an adequate assessment. Like the other models, a positive result indicates that investment should be pursued since the investment with the highest cost benefit is optimal.

- **Liabilities:** These are claims on the business. Claims are essential because many assets are obtained through purchase orders using payment schedules for which tracking and budgeting are important. The CISO must understand security program liabilities to provide appropriate accounting and financial support for the program.
- **Net Present Value (NPV):** NPV is the most complex analysis tool for comparing capital investment opportunities. It also offers the most precision. It is commonly used to analyze the profitability of a projected investment.
    - NPV indicates whether the projected earnings (or savings) a project or investment generates will exceed the anticipated costs in present dollars. Alternate models are required to communicate the *value* of a security project because security does not generate revenue. The NPV rule states that all projects that create a positive net present value should be accepted, while those that are negative should be rejected. If many items in the comparison have a positive NPV, the option with the highest NPV should be selected.
- **Profit and Loss (P&L):** P&L statements summarize an organization's revenues, costs, and expenses over a specific period. Depending on the organization and the purpose, the P&L can cover a month, a quarter, a year, or other accounting period.
- **Return on Investment (ROI):** This analysis tool with moderate complexity offers reasonable precision in terms of result. ROI is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of several different investments. It produces a ratio to measure the return relative to an investment's cost. A positive ROI ratio represents profit and indicates that the investment should progress. A negative ROI ratio represents a loss and suggests that the investment should be applied elsewhere. When comparing many positive ROI ratios, the asset with the highest ratio will return the most value to the organization and is the one that should be pursued.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Calculating the precise gain from an investment in the security program and the comparability of two projects is challenging. For example, different antivirus solutions may have the exact cost, but the gain varies between the solutions based on the features offered by the vendor.

- **Cost Avoidance:** CISOs have found that calculating costs that could be avoided through various aspects of the information security program is more advantageous than calculating an ROI. For example, avoiding the costs associated with fines and penalties for a data breach can prove more compelling than an ROI projection.
- **Revenue:** It defines the economic benefit derived from operating the business. In an information security program, revenue can be interpreted as the money generated from charging for information security services.
- **Expenses:** These refer to an economic sacrifice incurred in generating revenue. They are accompanied by decreased assets or increased liabilities resulting from consuming assets and services to produce income.

Organizations make economic sacrifices to invest in the security program as it is perceived as a cost of doing business. The cost of investing in the security program compared with the revenue traded for this investment can introduce negative perceptions about the security program. This is true if the organization sees something other than commensurate value from investing in security. CISOs need to manage this perception continually, showing the value of the information security program.

hide01.ir

1.3.1. Defining an Information Security Program Budget

Budgeting is an essential financial management process to estimate revenue and expenses over a specified period. Assessing and matching expenditures to income (actual or anticipated) helps determine whether enough money exists to fund operations or expand programs. CISOs can equate IS program revenue to annual funding and chargeback income from cybersecurity services.

Budgets are valuable because they demonstrate the trade-off made when one resource is exchanged **for** another. For the CISO, the security budget measures the exchange of financial allocations for the security products and services supporting the organization. To continue this exchange over the lifetime of the security program successfully, the CISO must manage the budget effectively. This will help determine whether the budget is in surplus, balanced, or deficit—which will assist in identifying appropriate adjustments. The budget managed by the CISO should do one of three things: increase revenue, reduce costs, or reduce risks.

1.3.2. Developing an Information Security Program Budget

When developing a budget, the funding level and when and how the funding is received will need to be **calculated**. This can be accomplished by sitting with the organization's chief financial officer (CFO) to understand how the program will be funded.

Financial objectives for the CISO are as follows:

- Understand how finances are managed in the business, especially in the security function.
- Consider other operating costs balanced with the financial strength of the business.
- Ensure that the cost of security controls cannot exceed the value of the protected

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information or assets.

- Understand and use standard financial management tools.

Two **principal** concepts in budget development are capital and operational expenditures, and CISOs need to understand the difference.

- **Capital Expenditure (CapEx):** CapEx is money a company invests in acquiring or upgrading fixed, physical, non-consumable assets such as buildings, equipment, or a new business. Regarding accounting, CapEx occurs when the asset is a newly purchased capital asset or an investment that improves the useful life of an existing capital asset. The CISO should consider all costs associated with a procurement activity when calculating the budget for CapEx. Overlooking delivery and installation costs can create a situation where the CISO has purchased a product or service, but funding is needed to deploy the solution properly.

  Capitalization includes all costs required to acquire an asset and should be considered when calculating CapEx. Capitalization helps the CISO avoid miscalculations when budgeting for an expense and helps to account for intrinsic costs like shipping, tuning, initial installation, or training to use the solution. The CISO should apply the concept of capitalization to everything required to support the successful delivery and building of the solution or service.

- **Operating Expenditure (OpEx):** OpEx accounts for all ongoing costs for running a product, business, or system. OpEx helps business leaders evaluate expenses resulting from normal business operations. A CISO must consider how operating costs can be managed without significantly affecting the mission and responsibilities of the information security program.

  When budgeting for OpEx, essential costs include salaries and benefits, equipment maintenance and service agreements, research and development, training, and outsourcing. Some CISOs also build **depreciation** into the budget to account for technology replacements, upgrades, and other unplanned expenses.

1.3.3. Managing an Information Security Program Budget

Financial management defines the processes of planning, organizing, directing, and controlling the monetary activities of an organization and the use of its funds.

The CISO plays a vital role in financial planning for the information security program. Because most funding for the security program is allocated from the organizational operating budget, the CISO has a fiduciary responsibility to be a good steward of the funds invested in the program. Achieving good stewardship requires an understanding of fundamental financial management concepts. This understanding promotes the economic success of the security program and its mission.

There are two standard methods of accounting for expenses in a security program. The CISO can use either a top-down or a bottom-up method. Each approach has advantages and disadvantages; the CISO determines the better method depending on the situation.

- **Top-Down Method:** The top-down approach starts by reviewing the total budget, including labor, materials, and other related costs. Next, the scope of each task is reviewed. Finally, a percentage of the total cost is allocated to each task based on the

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

size, resulting in a budget for each task. This method helps contain costs and prevents excessive spending. A disadvantage is that the total budget, if accurate, could result in more funding.

- **Bottom-Up Method**: The bottom-up approach starts by determining the specific costs of each task, such as labor, materials, and other related expenses. Next, the costs are totaled to establish a budget for each task. The sum of each task budget results in the total project budget. An advantage of this method is that it may help ensure sufficient funds for each task. A disadvantage is that individuals or groups within the company may overstate their actual needs, resulting in inaccurate budgeting.

1.3.4. Monitoring an Information Security Program Budget

Cash Flow: Cash flow measures the amount of money flowing into and out of a business. The budget is the best tool to manage cash flow and support the budget audit process. This provides an opportunity to confirm the validity of spending, which is critical for programs that do not generate revenue and have fixed budgets.

Burn Rate: This measures the rate at which the cash flows out of the business. Burn rate provides an effective method to evaluate and compare actual spending versus planned spending and helps to identify the extent to which actual spending deviates from planned spending. The usefulness of this analysis applies to all business functions in an organization that needs to track spending.

Burn rate is a typical analysis performed for fixed funding. The calculation supports efforts to ensure the speed at which money is spent is balanced with required financing. For example, the burn rate would identify that a utilization-based cloud contract is running out of funds because spending exceeds available resources for the activity.

It is vital to emphasize continuous monitoring and assessing the budget to detect variances, rectify cost overruns, and guarantee the efficient allocation of resources.

hidoc1.ir

1.4. Defining and Developing Information Security Program Staffing Requirements

Many critical activities in the security operations program must operate without interruption. This creates unique staffing requirements. The security operations staffing plan should define the operating hours for each activity within the program and ensure each has adequate personnel to support the operation.

A 2017 Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Survey of 126 healthcare organizations revealed the following staffing ratios [68]:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

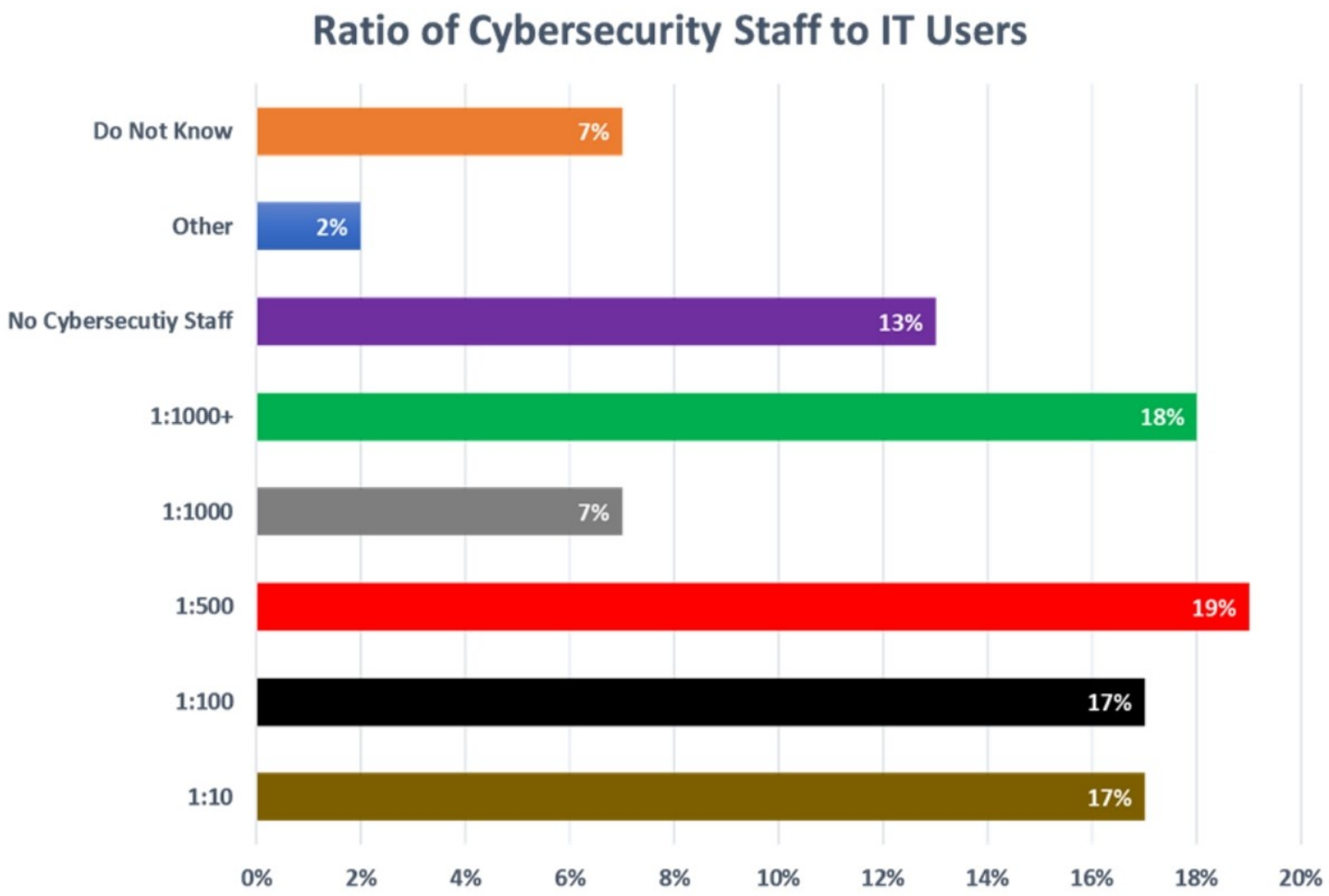


Figure 33: 2017 HIMSS Cybersecurity Survey—Staffing Ratios

The staffing plan should define resource availability from a 24-hour perspective and consider overlap and peak-time support arrangements. For example, the demands on operations staff may require four shifts instead of one using three eight-hour shifts. Additional shifts may be necessary to build downtime into the schedule of a demanding operations center, or personnel may require time considerations to support other activities in the program.

- **Administrative Staff:** Administrative personnel supporting the security operational program should possess analytical and communications skills. These skills contribute to the security operations program results communicated to the CISO, security program and project managers, and the broader organization. For example, communication within the security program differs from communication with other departments in an organization or external agencies. Administrative personnel should know how to tailor their communication to the intended audience.

- **Technical Staff:** Technical personnel who support the security operations program must understand how to identify, prioritize, and respond to security events in the organization. Technical operations responsibilities include designing security architecture, performing detailed log analysis, event management, incident response, and digital forensic investigations. In addition, technical personnel must understand how to use specialized tools that support security operations. They must understand how to process information provided by those tools and take appropriate action based on defined processes and risk management requirements.

- **Security Operations Staff**: Each program in the information security portfolio requires personnel with unique skills and capabilities. Personnel supporting the security operations program are essential. They have specific security qualifications, training, and certifications. Continuing education ensures they remain knowledgeable about security trends and are equipped to perform their duties. The knowledge and capabilities of these personnel heavily influence the effectiveness of, and the outcomes delivered by, the

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

security operations program.

- **Digital Forensics Staff:** Digital forensic investigation is a skill that requires extensive training and specialized software. The cost of supporting an internal digital forensics team leads some organizations to obtain support from third-party specialists when an investigation is necessary to support root-cause analysis or legal action. Contracts for forensic services can provide significant cost savings if this type of service is rarely required. This model also provides access to impartial expert witnesses if evidence from a forensic investigation is used in legal proceedings.
- **Interdisciplinary Skills:** In today's complex and interconnected threat landscape, effective security often requires collaboration with legal, compliance, and risk management functions. Security incidents may involve legal implications, regulatory compliance requirements, and risk assessment considerations. Therefore, integrating professionals within these areas into the security operations team can enhance the organization's ability to address multifaceted challenges. This collaborative approach strengthens incident response and compliance efforts and ensures a more holistic and strategic approach to security management.

1.5. Managing the People of a Security Program

Managing personnel within an information security program is the most challenging part of a CISO's role. This would be especially true if a CISO has never previously managed personnel. Many CISOs have emerged from the technical ranks where staff management experience is limited to small teams or a specific technical discipline. Within the information security field, technical people tend to be very independent, with many who find it challenging to respect managers who do not have the same level of technical ability. These reasons alone make it imperative that CISOs receive management training to improve their effectiveness.

To help CISOs manage people, the following tips will serve as a quick primer on employee management:

- Find what motivates each employee and use that as inducement for performing at their highest level.
- Apply positive corrective feedback to counsel employees who make mistakes.
- Challenge employees to surpass their core skills by learning new competencies so they can add value to other parts of the information security program.
- Give employees a voice in the information security program evolution.
- Provide a growth plan for employees, including training, certification goals, and a career path.
- Know when to manage problems with employees before they affect team morale.

1.5.1. Resolving Personnel and Teamwork Issues [69].

To manage conflict effectively, the CISO must be a skilled communicator and involve trained professionals from the HR department. Creating a conflict resolution strategy with the HR department ensures company policies are followed and minimizes the potential for a lawsuit. CISOs should have an open communication environment where employees can discuss work issues. Listening to employee concerns will foster a relaxed environment. It is important to

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

confirm understanding of what is said by asking questions and focusing on the employee's perception of the problem.

Whether it is two employees fighting for the desk next to the window or one who wants the heat on and another who does not, an immediate response to conflict situations is essential. Here are some tips that can be used when faced with employees who cannot resolve their conflicts.

UC Berkeley's Human Resources Manual suggests the following courses of action to resolve workplace discord:

- **Acknowledge that an inconvenient situation exists:** Honesty and clear communication play a significant role in the resolution process. The CISO must be aware of what is happening and be open about the problem.
- **Let individuals express their feelings:** Some feelings of anger and hurt usually accompany conflict situations. Before any problem-solving can take place, these emotions should be defined and acknowledged.
- **Define the problem:** What is the stated problem? What is the negative impact on work or relationships? Are differing personality styles part of the problem? Meet with employees separately at first and question them about the situation.
- **Determine the underlying need:** The goal of conflict resolution is not to decide which person is right or wrong; the goal is to reach a solution that everyone can live with. Looking first for needs rather than answers is a powerful tool for generating win-win options. To discover needs, the CISO must try to find out why people want the solutions they initially proposed. Once the advantages of their solutions have been understood, their needs have been discovered.
- **Find common areas of agreement, no matter how small:**
  - Agree on the problem.
  - Agree on the procedure to follow.
  - Agree on the worst fears.
  - Agree on some minor changes to give an experience of success.
- **Find solutions to satisfy needs:**
  - Problem-solving by generating multiple alternatives.
  - Determine which actions will be taken.
  - Make sure involved parties buy into actions. (Total silence may be a sign of passive resistance.) Be sure to get absolute agreement from everyone.
- **Determine the follow-up to monitor actions:** Suggest scheduling a follow-up in about two weeks to determine how the parties are doing.
- **Determine what you will do if the conflict goes unresolved:** If the conflict is causing a department disruption and remains unresolved, it may be necessary to explore other avenues. An outside facilitator (such as the Staff Ombudsman Office) can offer additional insights on solving the problem. Sometimes, conflict becomes a performance issue and may become a topic for coaching sessions, performance

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

appraisals, or disciplinary action.

1.5.2. Managing Training and Certification of Security Team Members

CISOs are responsible for ensuring program personnel have adequate training and the opportunity to achieve relevant certifications. The organization should pay for certifications to incentivize employees to improve their skill set. Some companies feel this works just the opposite, where they fear employees will leave after using all their training and certification budget. This is an old style of thinking and should be separate from the narrative of whether to offer paid training and certifications to employees.

CISOs must also have a succession plan for key personnel. Having cross-trained employees in core disciplines will limit disruptions if individuals leave the organization.

1.5.3. Clearly Defined Career Path

Members of the information security program should know how their careers will progress. It is crucial to structure job categories where employees know their achievements, time, and certifications will be rewarded. For example, if there is only one role called security analyst (SA), rather than SA 1, SA 2, and SA 3, staff will have nothing to aspire to within their career. It is also essential to show how employees can move from one role to another within the security organization. For instance, demonstrate the requirements to transition from SA to digital forensic analyst.

1.5.4. Designing and Implementing a User Awareness Program

Information security programs are only as strong as their weakest link, and that is the user community. Users can click on a malicious link, accidentally forward sensitive information, or delete critical information. Sometimes, security technology can overcome these everyday use mistakes, but often it cannot. The CISO must correctly train users of the organization's assets and information, avoiding risky actions that expose the organization to infiltration or privacy concerns.

Every organization must have a security awareness program to ensure employees know the importance of protecting sensitive information and identifying and avoiding social engineering attacks. Many regulations and standards mandate an effective user awareness program. Users tend to understand the importance of security when they understand the harm that could occur to the organization.

The following are the minimum requirements for a security awareness program:

- **Assemble the Security Awareness Team:** The first step in developing an awareness program is assembling a security awareness team to develop, deliver, and update the content. Organizational diversity in the team, where members come from various departments, is good practice.
- **Determine Roles for Security Awareness:** Designing awareness content specific to user roles is critical to program adoption and user interest. Material intended for administrative personnel should be different in some respects from materials oriented toward executives. For example, all employees should be trained in spearfishing attacks, and financial department personnel should be prepared to identify financial fraud.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Security Awareness Culture:** The awareness content and delivery method should also fit the organization's culture to be effective. When security awareness training is disseminated via multiple communication methods, personnel are exposed to the same information in diverse ways, reinforcing the message.
- **Define Metrics to Assess Awareness Training:** Metrics should be used to measure the success of a security awareness program. How the organization scores in areas of awareness will undoubtedly provide valuable information to keep the security awareness program up-to-date and effective.

1.6. Managing the Architecture and Roadmap of the Security Program

CISOs will be involved in developing the program's architecture and roadmap and managing the efforts of other's contributions. In this role, CISOs will serve as both designers and project managers. These activities cannot be done in a vacuum and should reflect consensus from stakeholders.

1.6.1. Information Security Program Architecture

The overall design of an information security program, depicting its structural components, interrelationships, and design principles and guidelines, is an architecture. It serves as a representation of what an information security program will look like when completed. It provides the vision of the program and is business outcome-based. The architecture has multiple layers, with each providing a different abstraction view. The architecture is also standards-based and includes the design requirements for building the information security program.

hide01.ir

The following are sources of information security program architectures:

- Department of Defense (DOD) Cybersecurity Reference Architecture [70]
- Open Enterprise Security Architecture (OESA) [71]
- Sherwood Applied Business Security Architecture (SABSA) [72]

1.6.2. Information Security Program Roadmap

Roadmaps are a vital means of visually conveying the information security program's goals and objectives. They offer a clear and concise method for articulating the program's strategic direction to its personnel, stakeholders, and sponsors. These roadmaps can encompass short-, medium-, and long-term perspectives, providing a valuable abstract overview of the program's strategic plan. It is important to note that roadmaps should be distinct from project plans but should maintain a broader perspective.

However, the imperative here is the need for frequent reviews and updates of these roadmaps. Rapid advancements mark the technology landscape, the threat landscape continually evolves, and regulatory frameworks undergo frequent changes. To ensure the relevance and effectiveness of the information security program, these roadmaps should be revisited regularly and adjusted to incorporate emerging technologies, respond to evolving threat landscapes, and remain compliant with the latest regulatory requirements. A pragmatic approach necessitates that the roadmap only extends up to three years, reflecting the dynamic nature of technology, threats, and regulations. Regular updates are the linchpin of a proactive and responsive security strategy in today's ever-changing cybersecurity environment.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is an example of a roadmap:

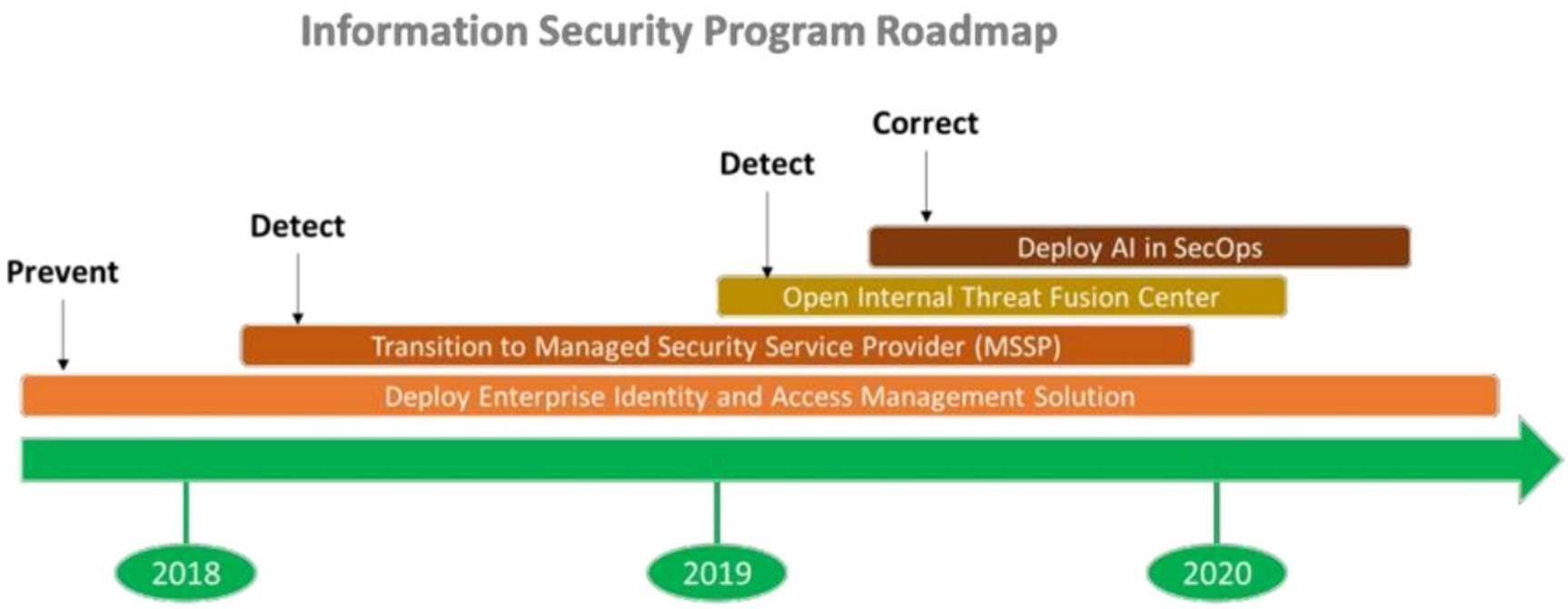


Figure 34: Information Security Program Roadmap

1.7. Program Management and Governance

Program Management encompasses an organization's endeavors to synchronize interconnected projects and initiatives to accomplish a particular objective or result. In contrast, project management involves supervising an individual task, focusing on successfully delivering the intended product, solution, or outcome.

What is Project Management?

Project Management develops and implements plans to achieve a specific scope driven by the objectives of its program and organizational strategy. It is primarily concerned with attaining specific deliverables that support specific organizational goals.

Effective project management influences the entire information security portfolio. A CISO must leverage project management to consistently deliver an organization's solutions, controls, and remediation. Otherwise, it becomes difficult to coordinate resources supporting the delivery of information security solutions and services on time and according to the project timeline.

1.7.1. Understanding Project Management Practices and Controls

The selected project management methodology will vary based on the size and scope of the project and the organizational culture that affects project management approaches. The traditional project management model includes five phases that divide project work into manageable and related activities supporting project delivery.

Project Management approaches follow similar methodologies, beginning with an initiation phase and finishing with the project closure. CISOs need to work with their organization's project management office (PMO) and understand how to use the PMO's project management methodology.

ride01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is a representation of traditional project management approaches:

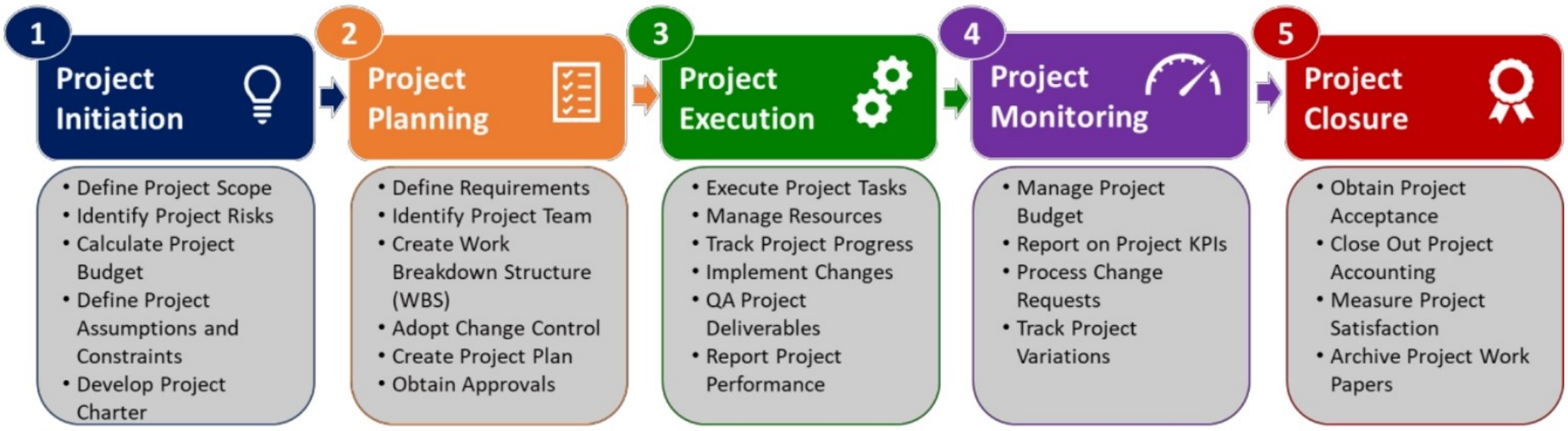


Figure 35: Project Management Life Cycle

- **Phase 1 - Project Initiation:** This first phase includes all activities required to approve and start the project. Prerequisites for initiation include a project feasibility assessment, identification of stakeholders, and identification of project constraints. These efforts provide input to create the project charter, formally creating the project.
- **Phase 2 - Project Planning:** Project planning exists to develop plans and documentation that define how the project will complete its work and deliver the proposed product or result described in the project charter. Two of the most important planning activities for a project include resource planning and documentation.
- **Phase 3 - Project Execution:** Project execution includes combining resources and plans to create the product or result as defined in the project plan. Project execution includes implementing numerous project controls to ensure the project follows the project plan. Controls include schedule, financial, project change, and quality.
- **Phase 4 - Project Monitoring:** Monitoring and control are sometimes combined with execution because they often coincide. As teams execute their project plan, they must constantly monitor their progress. To guarantee the promised delivery, teams must monitor tasks to prevent scope creep, calculate key performance indicators (KPIs), and track variations from allotted cost and time. This constant vigilance helps keep the project moving ahead smoothly.
- **Phase 5 - Project Closure:** A project is temporary. It has a defined beginning and end. Once it is completed, the project manager conducts closure activities. Project closure includes ending project activities and moving the result into its intended program. Lessons learned should also be captured as part of an organization's commitment to continuous improvement.

1.7.2. Identifying and Managing Project Stakeholders

The concept of stakeholders in program management also applies to project management. At the project level, a stakeholder is anyone interested in the project's outcome. It is essential to understand the stakeholders of a project and how they influence the project's outcome. Stakeholders can be internal or external:

iTeh01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

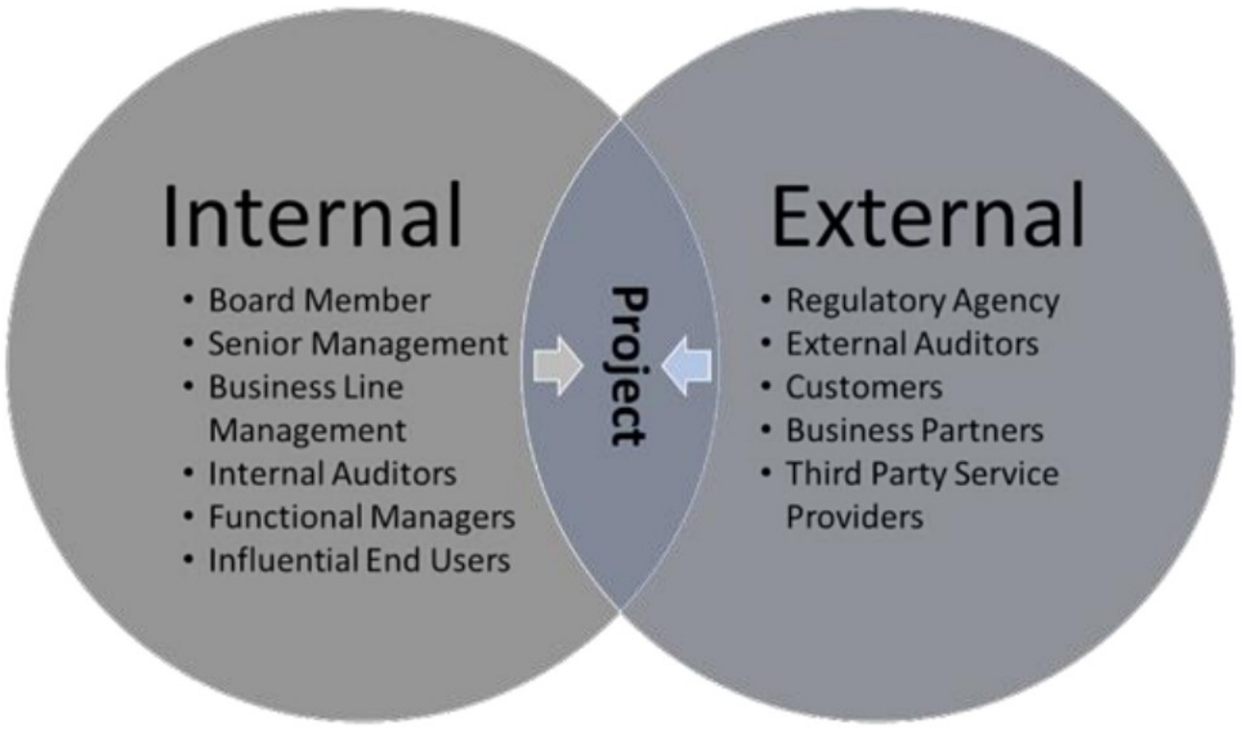


Figure 36: Project Stakeholders

Communication is the most important activity in stakeholder management. Stakeholders must understand and be informed of the project's progress.

1.7.3. Measuring the Effectives of Projects

Key Performance Indicators (KPIs) play an indispensable role in project management and aid in measuring the success or failure of project activities. Understanding KPIs and selecting the ones best suited to measuring a specific project team's performance is not always easy.

Here are some examples of the types of project management KPIs that apply to team performance and strength:

- **Financial:** These are typically utilized when the measure is monetary.
- **Quantitative:** These are used when the relevant metric is numerical or can be quantified. These metrics involve measurable quantities and are often expressed as numbers, counts, percentages, or other numerical values.
- **Qualitative:** Qualitative is used when the relevant metric is not easily quantified numerically. These metrics typically involve non-numeric attributes, descriptions, or qualities. For example, project quality ratings (excellent, good, fair) and brand perception (strong, neutral, weak).
- **Process:** A KPI evaluating the methodology employed in a project can be used when the priority is to assess efficiency.
- **Team performance:** This type of KPI can measure a team's strength and ability to execute.

KPIs measuring team performance are qualitative. However, a process or quantitative metric could also be used to evaluate teams—depending on the nature of the project, product, service, or industry—since the group and individual activities may involve using specific processes or quantifiable actions to accomplish goals.

nide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.8. Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)

CISOs are increasingly wearing multiple hats, including continuity of operations, which includes business continuity and disaster recovery. These disciplines are not mutually exclusive; one can only occur with the other if an organization desires to recover from a disaster event successfully.

1.9. Data Backup and Recovery

There are different methods of backing up an environment. The organization should choose the most appropriate method to support the governance strategy. The needs of the organization and recovery-time objectives (RTOs) are the primary drivers of this decision. CISOs must know that data encryption and encryption key management requirements for sensitive data must be considered for any implemented backup solution.

- **Tape Backup:** Tapes have traditionally been used for backing up systems and are still predominantly used due to their comparatively lower cost. This solution needs to weigh the low cost of the tapes against the ability to recover information promptly. For example, if the RTO is eight hours for a system and the recordings are in a storage facility three hours' drive away (with the tape-restore process requiring 10 hours), the objective will not be met. Having a disk solution on the premises with copy-to-tape created for offsite recovery can mitigate this; however, this requires additional hardware for the primary or recovery mirror sites.
- **Redundant Array of Independent Disks (RAID):** Various RAID implementations exist. The key concept is that information is written across multiple disks to provide faster read and write operations to and from the disk. RAID also offers varying levels of redundancy. This is helpful because another drive can provide the information if one disk fails.
- **Full Data Backups:** Full backups provide a copy of the data to a set of removable media for storage, preferably in an offsite location for disaster recovery. The backup contains copies of the contents of the data to enable full data recovery to a point in time.
- **Incremental Data Backups:** These backups record the data updates since the last full or incremental backup. These backups save space and time, as they do not back up the entire database or file. They are used with a full backup to restore to a more current point. The full backup and all the incremental backups since the full backup were taken are required to restore to the current point in time.
- **Differential Data Backups**: Differential backups include all the backups since the last full backup was taken. Since all the cumulative changes are stored, only the total and differential backups are required to bring the data to the current version.
- **Storage Area Network (SAN):** SANs are high-speed networks that combine various storage technologies, including tapes, disk arrays, and optical drives, that create a network-attached storage platform, which operates with the speed and efficiency of a locally attached drive. These devices can support disk mirroring, sharing data between network servers, and backup/restore operations.
- **Cloud Backups:** Cloud backup solutions have increased in popularity. These solutions can compress, encrypt, and store the data remotely for backup purposes. During a disaster,

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

data can be restored from cloud backups worldwide.

1.10. Backup Strategy

The Business Impact Analysis (BIA) is an essential first step in BCM because the analysis identifies the recovery point objective (RPO) and the recovery time objective (RTO) of each system or business process the organization uses.

- **Recovery Point Objective (RPO):** RPO identifies the maximum tolerable time limit in which data might be lost. This determines how much data the system can lose and defines the backup schedule.
- **Recovery Time Objective (RTO):** RTO identifies the duration of acceptable downtime. This determines how quickly the system or business process must recover and defines recovery priority.

BIA encourages active involvement and input from business leaders, IT, and security. Asset owners contribute by describing the business value of their systems. IT and security then transform this information into a prioritized plan to recover business processes and systems based on the context of their value and impact on business operations.

1.11. ISO BCM Standards

In addition to the standards for information security in the ISO 27000 series, the International Organization for Standardization documents important criteria for business resilience. The ISO BCM standards guide both a strategy and planning perspective and a technical recovery perspective.

The following are the most used business continuity standards:

hide01.ir

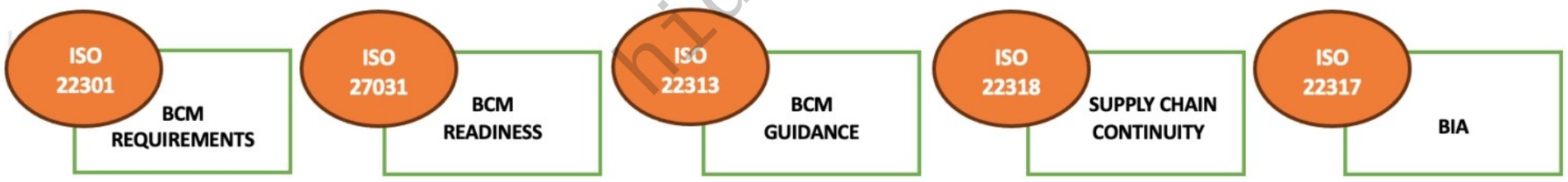


Figure 37: ISO Continuity of Operations Standards

ISO 22301:2019 | Security and Resilience—Business Continuity Management (BCM) systems—Requirements [73]

This standard specifies requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptive incidents when (or should) they arise.

The requirements specified are generic and intended to apply to all organizations, or parts thereof, regardless of the organization's type, size, and nature. The extent of application of these requirements depends on the organization's operating environment and complexity.

ISO/IEC 27031:2011 | Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity [74]

This standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity. It provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

implementation) to improve an organization's ICT readiness and ensure business continuity. It applies to any organization (private, governmental, and nongovernmental, regardless of size) developing its ICT readiness for business continuity program information and communications readiness for business continuity (IRBC) and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security-related) that could impact ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

ISO 22313:2020 | Security and Resilience— Business Continuity Management systems—Guidance on the use of ISO 22301 [75]

ISO 22313:2020 for business continuity management systems (BCMS) provides guidance based on good international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving a documented management system that enables organizations to prepare for, respond to, and recover from disruptive incidents when they arise.

It is not the intent of the standard to imply uniformity in the structure of a business continuity management system (BCMS) but for an organization to design a BCMS that is appropriate to its needs and meets the requirements of its interested parties. These needs are shaped by legal, regulatory, organizational, and industry requirements, the products and services, the processes employed, the environment in which it operates, the size and structure of the organization, and the needs of its interested parties.

nide01.ir

ISO 22313 is generic and applicable to all sizes and types of organizations, including large, medium, and small organizations operating in industrial, commercial, public, and not-for-profit sectors that wish to

- Establish, implement, maintain, and improve a BCMS.
- Ensure conformance with the organization's business continuity policy or
- Make a self-determination and self-declaration of compliance with this International Standard.

ISO/TS 22318:2021| Security and Resilience—Business Continuity Management systems—Guidelines for Supply Chain Continuity Management [76]

ISO/TS 22318:2021 guides methods for understanding and extending the principles of BCM embodied in ISO 22301 and ISO 22313 to manage supplier relationships. This technical specification is generic and applicable to all organizations (or parts thereof), regardless of type, size, and nature of business. It applies to the supply of products and services internally and externally. The extent of application of this technical specification depends on the organization's operating environment and complexity.

Supply chain continuity management (SCCM) considers the full range of activities concerned with providing supplies or services to an organization as a part of business-as-usual. The scope of this technical specification is less broad in that it considers explicitly the issues faced by an organization that needs continuity of supply of products and services to protect its business activities or processes and the continuity strategies for current suppliers within supply chains that can be used

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to mitigate the impact of disruption; this is SCCM.

ISO/TS 22317:2021 | Security and Resilience—Business Continuity Management systems—Guidelines for Business Impact Analysis [77]

ISO/TS 22317:2021 guides an organization to establish, implement, and maintain a formal and documented business impact analysis (BIA) process. This technical specification does not prescribe a uniform process for performing a BIA but will assist an organization in designing a BIA process appropriate to its needs.

ISO/TS 22317:2021 applies to all organizations regardless of type, size, and nature, whether in the private, public, or not-for-profit sectors. The guidance can be adapted to the organization's needs, objectives, resources, and constraints. It is intended for use by those responsible for the BIA process.

1.11.1. Business Continuity Management (BCM)

When IT operations or the cybersecurity program is in recovery mode, the organization must continue to provide critical business functions. These functions can continue using third parties or semi-manual approaches. In extreme cases, the organization can invoke a temporary cessation of activities. This subcomponent aims to make the organization resilient to disaster events.

Business continuity planning (BCP) ensures that business operations can continue successfully through a business disruption. The activity consists of several steps that equip an organization to document formal plans and procedures required to restore operations. The plan's scope can focus on a single process, system, business unit, or organization. Each plan combines analysis from the BIA with consideration of the procedures required to restore operations after a disruption.

The complexity of the BCP depends on the supported activity. For example, continuity planning for a business process or a single system will be more focused and less complex than the plan for all operations in a business unit—or a plan for the entire enterprise. Plans can include content such as requirements for HR, food, safety, transportation, security, and manual procedures for continuing service to customers during the disaster event.

The following checklist highlights recommendations for content to consider in a BCP regardless of the scope or the activity supported:

- BCP roles and responsibilities
- Lines of authority, succession of management, and delegation of authority
- Notification roster and call trees for key personnel and external partners
- Communication plan for external customers and support organizations
- RPO and RTO from the BIA
- Detailed procedures, resources, and logistics for recovery of processes and systems
- Procedures for manual alternatives to automated processes
- Test plans and training exercises
- Schedules, triggers, and requirements for plan maintenance and updates

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Continuity planning is flexible and customizable. Organizations should tailor the BCP to address unique concerns identified in the BIA and document the necessary information to support restoration after a business disruption. They should also ensure the plan is accessible and distributed to appropriate personnel to guarantee that the BCP is available to the right people when an event occurs.

1.11.2. Disaster Recovery Planning (DRP)

Disaster recovery focuses on the technical recovery of systems and solutions that support an organization. The DRP traditionally focuses on the activities required to restore systems to an operational state after a contingency event occurs. Execution of the DRP ensures that the computing infrastructure is recovered to a point where the business can continue to run, even if those operations occur at an alternate processing site.

Because DRP focuses on the technical recovery of systems, formal documentation of run books and detailed instructions for bringing systems online are critical. During a contingency event, the personnel who recover the system may be different from the personnel who usually support the system. This lack of system awareness makes documentation of the installation procedures critical. In addition, to support effective recovery, the organization must ensure that system changes trigger updates to the processes that document recovery.

The restoration of systems to an alternate processing site constitute a common strategy that supports BCM. Organizations can set aside space in their facilities to help alternate processing or partner with another organization that provides an alternate site. The three common sites for alternate processing include hot sites, warm sites, and cold sites. Each type has unique benefits and considerations that organizations must evaluate to identify the best solution to support BCM requirements.

There are several alternate recovery site configurations available for CISOs to select from:

h1de01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Alternate Site	Overview
Disaster Recovery as a Service (DRaaS)	DRaaS fails over processing to the cloud so an organization can continue to operate during a disaster. The failover notice can be automated or manual. The DRaaS operation remains in effect until IT can repair the on-premises environment and issue a failback order.
Hot Site Recovery	Hot sites are fully operational facilities for alternate processing. The environment is compatible with the environment that is being backed up and includes the necessary network, systems software, and infrastructure. It can be ready to assume normal operations of the organization because the latest version software, systems, and data are available at the site. This is the most expensive solution for alternate processing, but hot sites have the shortest recovery time.
Warm Site Recovery	Warm sites have the basic infrastructure of cold sites, but with the installation of sufficient systems and communications to operate at the site. Warm sites and hot sites differ regarding the software and data loaded at the sites. Warm sites have systems in place, but require data recovery from backup media to support normal operations. These sites often have the capacity to run critical systems during a contingency event, but do not have the resources required to run all systems. Warm sites support expedited, not immediate, recovery at a moderate cost that is higher than that of a cold site, but more economical than that of a hot site.
Cold Site Recovery	Cold sites have basic infrastructure and environmental controls like electricity, heating, ventilation and air-conditioning (HVAC), and wiring. This type of facility has no equipment or telecommunications in place; therefore, it will take longer to bring the site online and restore operations. Organizations often limit the use of cold sites to emergency restoration of critical system functions. This is the least expensive solution for alternate processing, but cold sites have the longest recovery time.
Mobile Site	Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements. These sites are often available as trailers that are pre-configured with equipment. They can be deployed anywhere and become operational quickly, which is valuable as part of the recovery plan associated with widespread natural disasters. The cost of mobile sites depends on the size and capability of the site requested. Costs also vary regionally based on the vendors who are available in a particular location to configure and deliver the sites.
Redundant Sites	These facilities may be used to house a few critical applications that need to be up quickly. Systems may load share or fail-over automatically to the backup site. These are used in situations where high availability is important, as these sites are the most cost intensive because of the requirement for completely up-to-date information. These are also called "mirror sites" because they are completely updated and can take over processing without a loss in service. An organization may build a test environment that is configured the same way as the production environment for use during a disaster.

Table 19: Alternative Recovery Site Overview

Appropriate agreements should exist to ensure that any partners that support operations at an alternate processing site can provide the resources necessary for success. When disasters occur in a region, there will be competition for disaster recovery resources, and an organization needs to understand the probability that its services will receive priority. A larger organization with multiple data centers can better accommodate the recovery effort if they have the infrastructure and resources available to support the disaster recovery team.

Organizations must ensure that the recovery strategy provides a solution that meets an organization's risk profile. The security safeguards at the alternate processing site require evaluation to ensure that information and assets at the location are protected at the same level offered at the primary site.

Single points of failure (such as telecommunication services and utilities like power, gas, and water) should be noted at the alternate processing site. Where feasible, organizations can manage their way through disasters with a multilayered approach to the primary data centers with dual power lines, telecommunication providers, and backup generators to keep the system operational where most appropriate.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.12. Continuity of Security Operations

An organization should determine whether information security continuity is captured within the BCM or disaster recovery management processes. Information security requirements should be determined when planning for business continuity and disaster recovery. Without formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations compared to normal operational conditions.

The organization should establish, document, implement, and maintain processes, procedures, and controls to ensure the required continuity for information security during an adverse situation.

To reduce the time and effort of an *additional* business impact analysis for information security, capturing information security aspects within the normal BCM or disaster recovery management business impact analysis is recommended. This implies that the information security continuity requirements are explicitly formulated in the BCM or disaster recovery management processes.

1.12.1. Integrating the Confidentiality, Integrity, and Availability (CIA) Model

The CIA model is ideally suited to ensure recovery operations are adequately secured from security breaches.

- **Confidentiality:** Backup data must stay confidential, including data encryption, if production data is encrypted to prevent accidental disclosure during recovery.
- **Integrity:** Ensuring that the correct backups are used for recovery is crucial to the integrity of the recovery processes.
- **Availability:** All recovery and business continuity resources must be available anytime to support the recovery event.

hide01.ir

1.13. BCM Plan Testing

It is important to test the recovery plan to ensure its effectiveness. Periodic testing must occur to increase the probability of successful restoration during a disaster. Increased levels of confusion and anxiety may occur during a disaster, leading to variances from the plan or unforeseen problems. However, testing BCM plans and practicing execution increases successful recovery opportunities during an event.

There are several methods for testing, ranging from basic tests involving minimal expense to full-blown tests, where the operations are intentionally interrupted. The following tests are in order of difficulty and expense:

- **Test Plan:** A thoroughly documented test plan should be implemented to ensure a recovery test does not manifest into a disaster. Test plans identify a test's resources, time limits, and recovery objectives. They provide a baseline to gauge the effectiveness of the test results.
- **Checklist Review:** The disaster recovery planner validates the checklists of the resources required for the recovery with the disaster recovery team. The checklists include the items needed to recover, such as the software, hardware, people, plans, telecommunications, procedures, and space. Missing a critical software component can cause delays in the recovery effort or, at worst, make the recovery of a system infeasible.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Tabletop Walkthrough:** The team reviews each step of the plan to evaluate its correctness and viability. Changes to the plans are discussed, and plans are updated. The team reviews the plan to see if it applies to existing systems. The walkthrough also familiarizes people with the plan, its location, and its responsibilities in the event of a disaster. The disaster recovery planner may be intimately familiar with the plans, as that is their primary role. Still, a successful recovery will depend upon all the participants from the other parts of IT and business organizations who need to implement and verify the recovery results of the plan.
- **Simulation Test:** The team role-plays a disaster and conducts the strategy without declaring a disaster or using the recovery site. The test scope may be limited to a program, department, or enterprise. This mock test can cause people to think of items that may be missed while they relate this to a real-life scenario.

1.14. DRP Testing

As with BCM Plan Testing, DRP testing is a crucial aspect of ensuring that the plan is effective, and that the organization can successfully recover from different types of disruptive events. The following are types of DRP tests:

- **Parallel Test:** This type of test compares the recovered solution to business-as-usual processing over a period to ensure that the assumptions made in the data collection for the disaster recovery are correct. The recovery site becomes operational, and the normal site continues as usual.
- **Complete Interruption:** Production is shut down from the primary site, and operations are moved to the recovery site for processing. Because this can be extremely expensive and disruptive to business operations, this type of test is usually not performed on a large scale.

1.15. Contingency Planning, Operations, and Testing Programs to Mitigate Risk and Meet Service Level Agreements (SLAs)

Any disruption to IT operations can impact an organization's service level agreements and contractual commitments to partners and customers. A fundamental way to limit disturbances and reduce risk is to ensure that the organization's contingency plans and practices are adequately evaluated. Containment plans are necessary for an organization's risk mitigation strategy, whether the threat is logical or physical.

The SLA clock begins with the first minute of a disruption. With that in mind, CISOs should counsel contract managers on how to craft an SLA based on the estimated timeframes of restoring business operations. For example, if it takes four hours to restore customer service, an SLA should reflect that fact before penalties accrue. Testing contingency plans is essential to build confidence in business restoration timelines. As crucial as SLAs are, managing or mitigating impacts is equally important as SLAs are based on impacts. Risk management and SLAs are inexorably linked, which means CISOs and contract managers must be in lockstep when SLAs are first drafted.

1.16. Computer Incident Response (aka Cyber Incident Response)

Incident response requires a comprehensive approach that begins with defining and categorizing incidents. Categorization provides an opportunity to respond appropriately when various categories of incidents are reported. The policies and procedures that govern incident response

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

will determine the organization's actions and processes to contain threats, apply proper mitigation, and restore systems to their normal operating modes.

1.16.1. Incident Response Tools

Security information and event management (SIEM) supports identifying events and incidents. The CISO should also consider other tools to help response and recovery activities. Common considerations include laptops with security analyzer software, packet sniffers, protocol analyzers, forensic workstations, storage and replication solutions, and networking equipment to evaluate scenarios and provide means to restore files. The considerations should include nontechnology resources like notebooks, evidence tape, tags, and bags to support response and investigation activities.

1.16.2. Incident Response Management

Incident analysis forms the basis of an organization's ability to respond effectively to cybersecurity incidents. Computer security incidents are often complex, multifaceted problems that require advanced analysis of technical details to understand what happened, find the root cause, and identify remediation steps necessary for recovery and response.

The analysis requires experienced personnel to consolidate all the data points related to the incident. The correct data must be collected from suitable sources. Information provided during the initial analysis provides a roadmap for additional data-gathering efforts. Determining the root cause may lead one to identify weak or ineffective organizational controls. This may require coordination with other programs within the information security portfolio or other parts of the organization (such as Governance and IT).

The analysis aims to identify an incident's impact and appropriate escalation to support timely remediation. The effect will define the response priority for the incident within the context of other events and incidents the security operations team is managing.

1.16.3. Incident Response Communications

- **Internal Incident Communication:** Effective internal communication is also essential to keep personnel informed, reduce stress related to the incident, and reinforce policies and standards for external communication.

  This reinforcement is necessary as personnel may need to remember the external communication policy during an incident so as not to unintentionally disclose harmful or erroneous information. Depending on the type of incident, inappropriate disclosures from employees can worsen the situation. For example, improper communication on social media about a breach or incident could result in unnecessary and additional attention from external regulators.

- **External Incident Communication:** External incident communication is essential. Organizations should develop a strategy that addresses communication with law enforcement to support any legal action or criminal investigations associated with an incident. Organizations should also plan communication with the media to support an effective public relations strategy related to an incident.

- **Law Enforcement:** Law enforcement can provide resources to investigate incidents and provide intelligence information. The Federal Bureau of Investigation (FBI), Secret Service, District Attorneys, and various state and local law enforcement agencies

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

can support the security program in the United States. Intelligence units collect information and provide analysis, storage, and provision of intelligence to authorized parties. Outside the United States, international agencies like the International Criminal Police Organization (Interpol) and the Law Enforcement Intelligence Unit (LEIU) work with a country's law enforcement agencies to support incident investigations and information sharing.

The operations staff needs to understand the thresholds or types of incidents for which they would engage law enforcement agencies. Law enforcement can provide a wide range of assistance, such as guidance for maintaining the chain of custody and presenting facts in court. Leveraging this experience can make the security program policies and procedures more effective. Operations staff would engage with external parties only under the guidance of the incident response team management.

- **Media Relations:** Some incidents may attract media attention and require procedures for handling media inquiries, press releases, and interviews. Improper media communication can create problems for public relations and legal proceedings when released information needs to be completed, corrected, or understood. A single spokesperson with input from the CISO, technical personnel, legal counsel, and public relations should interface with the media.

  Planning for the message and talking points is critical for effective communication. Personnel in the organization should understand policies and procedures related to communicating with the media. Some organizations expressly prohibit communications and restrict interactions to a public relations or media relations department.

1.16.4. Post-Incident Analysis

Each new incident provides the opportunity to gain experience. Post-incident analysis offers a chance to evaluate the organization's event management and incident response procedures. Further information from each recent incident should be part of every incident response process. A meeting after the event is addressed allows program staff to document root causes and lessons learned and revise processes to support continuous improvement. The CISO should ensure that new information from each incident response activity is incorporated into the policy and procedures to improve the incident response process.

1.16.5. Testing Incident Response Procedures (aka Playbooks)

Testing incident response plans are equally important to evaluating a DRP or penetration testing web-facing applications. Incident response team members must rehearse how they will react to several scenarios to perform their roles effectively.

The following checklist can aid in the formulation and execution of an incident response test:

- Select a scenario that poses the most significant risk to the organization.
- Add as much realism as possible to the test.
- Ensure incident response team members only use procedures documented in the incident response plan.
- Document plan changes identified during the test.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Determine if cross-training is necessary to ensure the plan does not rely on a single person.

1.17. Digital Forensics

Digital forensics ensures documentation of a systematic investigation and preservation of evidence with an appropriate chain of custody. Forensics is responsible for profoundly analyzing a security event after the fact. The digital forensics process goes beyond incident response procedures and helps an organization identify the events in an incident. This information is helpful in root-cause analysis, facilitating improvements in controls or business processes. In addition, the information supports legal proceedings if the investigation provides enough information to identify the attacker.

1.17.1. Digital Forensics Life Cycle

The National Institute of Standards and Technology (NIST) defines four phases supporting digital forensics: collection, examination, analysis, and reporting [78]. Each phase describes distinct activities that contribute to the success of the digital forensic investigation process.

The following framework will guide you in formulating your information security program's digital forensics program:

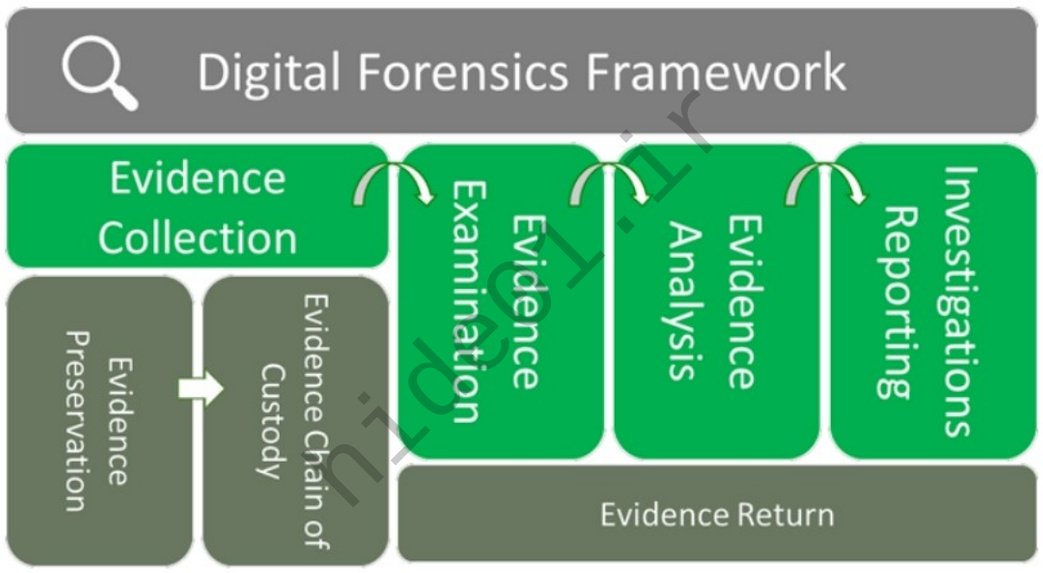


Figure 38: Digital Forensics Framework

The following describes each of the components of the digital forensics framework:

Evidence Collection: Collection is the most critical phase of the digital forensic investigation process. The organization must determine the investigation's intent before starting the collection process. Conceptually, preservation of evidence and chain of custody constitute the base of the forensic investigation structure. These are foundational concepts. Forensic investigation requires the collection of information as broadly as it makes sense. The data is refined to find what is most relevant while moving through the rest of the process. The investigation cannot be improved at later phases if there are problems with the collection or the chain of custody at the onset of the investigation.

- The Scientific Working Group on Digital Evidence (SWGDE) defines best practices to support the logical and physical acquisition of computers and their associated storage media for investigation. This guidance assists examiners in a lab setting and personnel who collect digital evidence in the field to achieve consistent collection for all investigations.
- Consult with the investigator to determine the details of the case and potential evidence to be collected.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Determine the necessary equipment to take to the scene.
- Review the legal authority to collect the evidence, ensuring any restrictions are noted. If necessary, obtain additional authority for evidence outside the original scope during the collection.
- All individuals not involved in the collection process should be removed from the proximity of digital evidence.
- Individuals with relevant information (usernames, passwords, operating systems, and network credentials) should be identified and interviewed.
- The scene should be searched systematically and thoroughly. Searchers should be able to recognize several types of devices that may contain digital evidence (for example, novelty USB drives, servers, and wireless storage devices).
- The possibility of anti-forensics techniques (destructive devices and wiping software) should be considered.
- Occasionally, there may be a need to conduct traditional forensic processes on media (for example, DNA and latent prints). These are case-dependent and should be discussed with the investigator to determine the need for such processing and the order in which the processes should be performed.
- When evidence from the scene cannot be removed, it should be copied or imaged on-site.
- A good practice of evidence collection is to take digital images (video or photographic) of the work area of the affected equipment when possible. Particular attention should be paid to area access, visible/accessible login credentials, screen status, etc.
- Standardized forensic software that has demonstrated admissibility in a court of law should be used.

hide01.ir

Chain of Custody: Each collection step and all interactions with the evidence must be recorded to maintain the chain of custody. Chain of custody refers to the documented record that provides accountability for each step of the handling process. The forensic investigation process must demonstrate that information handling procedures and actions performed did not alter the original data throughout the custody chain. This may include the following:

- Recording the name and contact information of those charged with maintaining a chain of custody
- Details of the timing of the event
- The purpose for moving the data
- Identification of evidence through recording of serial numbers and other details
- Sealing the evidence with evidence tape
- Documenting the location of storage
- Documenting the movement of the information

Evidence must be dependable to support legal proceedings or root-cause analysis. Policies, procedures, and training are recommended to ensure the chain of custody is understood and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

applied correctly to each investigation.

Evidence Preservation: The key to collection and preservation is to collect data to prevent accidental changes. Plans should exist that define how to acquire data and the method used to copy data. The data should be replicated using defined processes and tools to ensure the original evidence is not modified. Logs of observations and pictures or videos of the collection process should be kept, verifying further that tampering was not introduced to the evidence. Severing network connections and powering down the affected host must be done carefully to ensure these activities do not destroy valuable data required to support investigations.

The process must prove that data collected on day one has not changed when analyzed later—nonrepudiation. The file format used for collecting evidence should make it hard to change it without destroying the file. This is akin to creating evidence containers (logical file structure) that prevent the data from changing once it is in the container. This also protects the data from manipulation or change when it is being evaluated.

Evidence Examination: The second phase of the digital forensics process is examination. Files marked for further analysis are determined during this phase. Only some of the information collected will be of value, and the role of the analyst is to sift through the information, typically with forensic tools operating on a copy of the original data. While searching through various files and formats, tools are used to search and locate documents with key phrases or patterns. The data may have to be restored to another device from the backups to perform this analysis.

Special issues arise with encrypted files. The encryption method may need to be determined from the file header, and the file may be decrypted if the encryption method is weak or if the decryption key is located on other media. The primary objective of this phase is to reduce the available evidence to that deserving more detailed analysis.

nidem.ir

Evidence Analysis: The third phase of the digital forensics process is analysis. The analyst inspects data during this phase to determine the activities that occurred in terms of the following:

- Who was involved?
- What occurred?
- When did the events occur?
- Where did the action originate, and where was the impact?
- How was it accomplished?

The analyst's job is to gather information by examining and correlating disparate sources of information. SIEM tools can automatically correlate some of this information, provided the organization configured the system to do so with logs of the systems. Intrusion detection systems can assist in analyzing network activity and individual hosts, where activity logs can be further examined along with user events through their account or email system. The forensic analyst can review documents, spreadsheets, graphics files, and other information to construct a timeline of events. Each step of the analysis process should be recorded with the date and time of its completion.

Investigation Reporting: The final phase of the digital forensics process is reporting. A report with the information collected with event descriptions is created in this phase. The

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

analysis steps support the conclusions, and the report is written clearly so it can be understood by the audience receiving it. There may be multiple levels of information, including an executive summary or presentation for organizational leaders highlighting important items from the detailed reports. The methodology used to perform analysis and determine the results should be provided. Recommendations for mitigating issues found during the analysis should also be noted.

Reviews can be conducted to discuss improvements to policies and procedures and additional investments to the infrastructure in support of the program. This could include the capability to capture more source data, purchase different forensic tools, add file retention capabilities, increase storage, or provide additional forensics training.

Evidence Return: The returning of digital evidence requires handing back the physical and digital sources to the rightful owner.

2. OPERATIONS MANAGEMENT

2.1. Establishing and Operating a Security Operations (SecOps) Capability

Security operations is one of the most important programs within the information security portfolio. This program orchestrates people, processes, and technologies to provide the capabilities of an organization to deliver security services such as event identification, incident response, and digital forensic investigations.

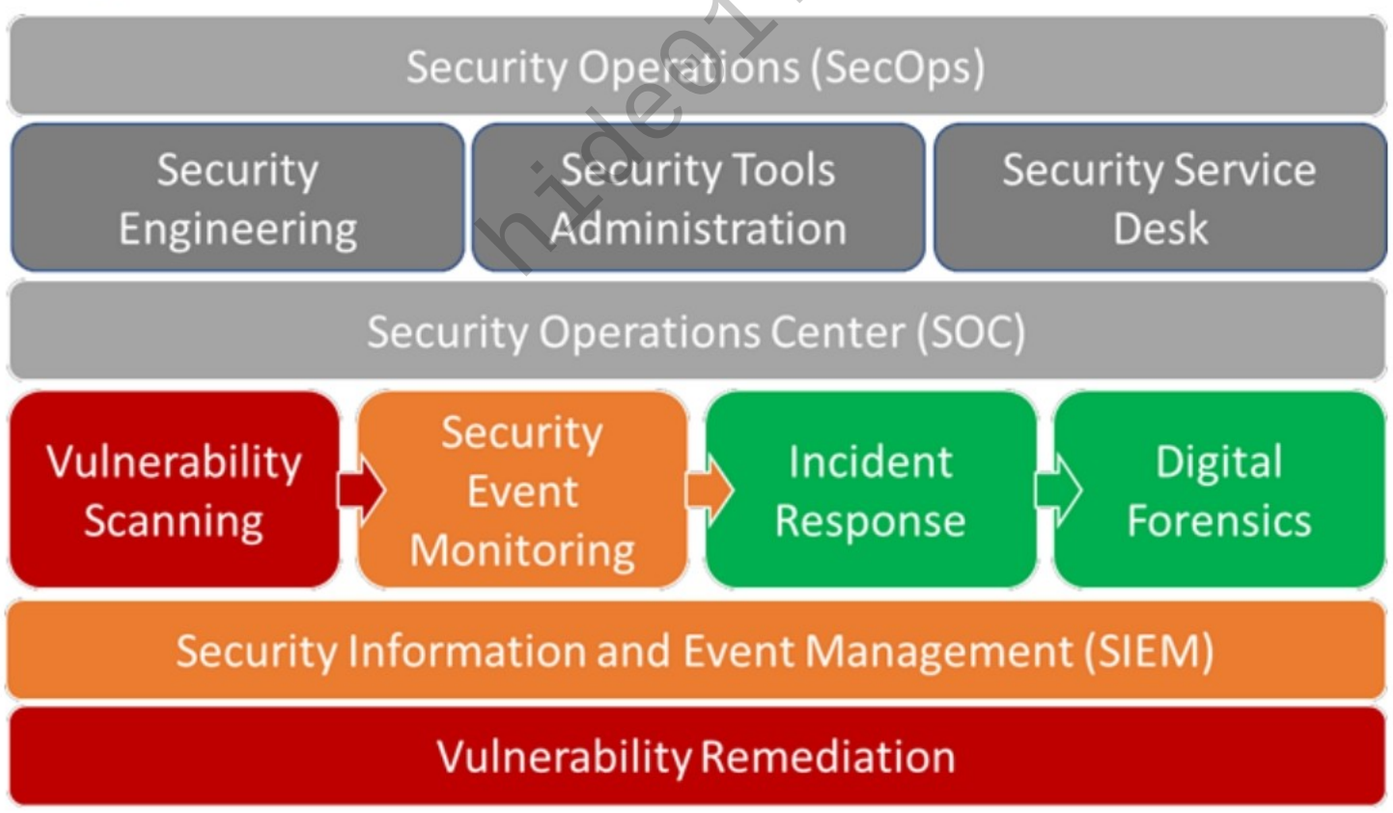


Figure 39: SecOps Framework

The security operations program can be as broad or narrow as required to satisfy the organization's security requirements. Factors such as corporate culture, executive support, financial constraints, and regulatory requirements influence the design and complexity of the program.

Security Engineering: Security engineering defines the organization's protection strategy and activities. It also works to ensure this strategy is incorporated into those activities. The resources for this activity include selecting and implementing technical, managerial, and organizational controls to protect the organization and its business processes.

This group should have dedicated resources to collaborate with other organizational units to build

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

security into business processes and applications and develop enterprise-wide controls in coordination with IT. The security engineering team should work closely with the corporate acquisitions program. From an acquisition perspective, the security engineering team can provide valuable insight into the security of products and services considered for procurement. The security engineering team should work closely with the enterprise architecture program. The team should also work closely with the application development program to facilitate security testing throughout the systems development life cycle (SDLC) phases.

Top 10 Security Engineering Principles [79]

The Engineering Principles for Information Technology Security defined in NIST SP 800-160v1 presents a list of system-level security principles to consider in designing, developing, and operating an information system. Ideally, the principles presented there, of which the top ten are listed, would be used from the onset of a program and employed throughout the system's life cycle. These principles are also helpful in affirming and confirming the security posture of already deployed information systems:

- Principle 1: Establish a sound security policy as the *foundation* for design.
- Principle 2: Treat security as integral to the overall system design.
- Principle 3: Delineate the physical and logical security boundaries governed by associated security policies.
- Principle 4: Ensure that developers are trained to develop secure software.
- Principle 5: Reduce risk to an acceptable level.
- Principle 6: Assume that external systems are insecure.
- Principle 7: Identify potential trade-offs between adding security and user functionality.
- Principle 8: Implement tailored system security measures to meet organizational security goals.
- Principle 9: Protect information while it is being processed, in transit, and storage.
- Principle 10: Consider custom products to achieve adequate security.

hide01.ir

The principles are valuable from all perspectives, US and international, because they map to the Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems. This mapping provides a foundation to define universally accepted guidelines for building security into programs, products, and organizations.

Security Tools Administration: This refers to tools required to provide daily operations support of cybersecurity technology and troubleshooting operational issues.

Security Service Desk: This team provides user support for cybersecurity program technology, user device virus infections, and access administration.

2.2. Security Monitoring and Security Information and Event Management (SIEM)

SIEM is the primary tool used to support the security operations program in large enterprises. Organizations with the resources to support this tool can manage the SIEM as an activity within the security program. Because of the cost involved, some organizations leverage services a

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

managed security service provider (MSSP) offers to provide operational support for the SIEM. In contrast, the organization provides administrative support and oversight for the activity.

- **The underlying principle of a SIEM:** The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations, and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.

SIEM is an effective tool to expand and enhance event and incident management support. The tool collects relevant information as feeds from other devices and endpoints in the enterprise and provides perspective about this information from a central repository or console. Manual collection of event information in the enterprise is not feasible because of the volume of data involved. Data collection usually involves data consolidation in a database with information from nodes throughout the enterprise. The SIEM analysts' normalization and correlation function provides pinpoint actionable events and responds appropriately to support remediation.

- **SIEM Use Cases:** Developing use cases can enhance the value of SIEM by providing a structured approach to test processes, evaluate detection and response capabilities, and train personnel.

Developing SIEM Use Cases [80]

A use case is typically developed in a complete process, not just as a simple task. The process has several stages:

- Define the requirements for the use case and identify the intended outcome.
- Define the scope of the requirement.
- Validate event sources that support the expected use case function.
- Define the logic of the alert and the associated attack vector.
- Conduct implementation and testing to confirm that the SIEM produces the intended result.
- Define use case response procedures.
- Conduct maintenance to support continuous improvement and tuning.

The effort applied to develop and evaluate the scenarios will help confirm assumptions about the program's understanding of the environment it supports. Testing use cases can also uncover previously unidentified vulnerabilities. For example, a test scenario that involves the intrusion detection system may disclose an unpatched system that requires remediation.

2.3. Event Management

Event management follows a system process from monitoring or searching for events to classifying events.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 40: Event Management Model

- **Event Monitoring:** Modern IT environments present a challenge for event monitoring due to the volume of information flowing within them. Data management discipline is critical because even with automated tools, assimilating and deriving meaning from a large volume of data is difficult.

  The CISO must ensure the following processes are implemented to support effective event monitoring and detection via automated tools:

  - Security logs must be consolidated and maintained. A strategy for storing and preserving log files must be defined and implemented.
  - Events must be aggregated, normalized, and analyzed consistently to provide a baseline for normal activities within the enterprise.
  - Alerts must be generated and routed to appropriate individuals when suspicious or anomalous activity has been identified. The incident management process must be activated if the event represents an imminent security threat.

- **Data Collection:** Data collection describes the systematic approach used by the organization to gather timely and relevant information about events in the enterprise. The CISO must develop a strategy to collect adequate information to support analysis and identification. Data has limited value if it does not contribute to developing an understanding of events. Data collection will vary among organizations depending on the objectives and priorities of the security program. Event use cases designed for the security operations program can provide a starting point to identify the information an organization needs to collect.

- **Data Normalization:** Normalization is a process that transforms data from disparate sources and reorganizes the data so that the data is consistent and the dependencies and relationships within the data are logical. Normalization allows analysis and identification tools to use standardized queries to evaluate data from multiple sources and isolate anomalous or malicious activity signs. Because normalization transforms data, the CISO should develop a strategy to archive the original data for additional investigation and forensic analysis. The actual data to detect an event may be needed as evidence for further actions.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Data Correlation:** Correlation defines the process of identifying relationships between data. Normalization transformed data from disparate sources, whereas correlation provides significant value by identifying relationships between events on different devices throughout the IT infrastructure. Data feeds offer information that can enhance the correlation process to identify associations between events and attack patterns. The results of data correlation provide visibility and allow the security operations team to identify and respond to events based on data relationships.

  Event correlation often requires tuning by an experienced analyst to reduce false positives and increase system effectiveness. A new implementation will often create alerts for regular traffic because excessive traffic on a network can exceed the predefined threshold in the correlation rules. Periodic reassessment and reevaluation are recommended to ensure the correlation implementation supports the event management strategy.

- **Data Retention:** CISOs must determine how long data should be retained to meet legal and regulatory requirements. A data retention schedule is required to guide employees and data custodians on the duration data should be included in a state where it cannot be altered, lost, or destroyed.

- **Event Identification:** Identification depends on learning the nature and relevance of an event and discerning its criticality at an early stage. Identification provides the first opportunity to categorize events at the end of the preliminary analysis. The CISO must define the criteria that distinguish an incident from an event. Identifying the type of event and assigning a category supports the subsequent steps in the event management and incident response processes.

- **Event Classification:** This is often based on the type and impact of the threat. It includes assessing, prioritizing, and relating events to other potential incidents and events. With proper context, events can be categorized based on criticality, impact, and relationship to other ongoing events managed by the security operations team.

  Organizations should define event and incident categories to support identification and management processes. Customization is vital to ensure the categorizations relate to the organization's priorities. The table below provides an example of events and incidents defined by the U.S. Department of Defense. The table highlights the value of categories mapped to describe the event or incident.

The following is an example of event categorization:

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Reportable Event Categories	
Category	**Description**
0	Training and Exercises
1	Root-Level Intrusion
2	User-Level Intrusion
3	Unsuccessful Activity Attempt
4	Denial of Service
5	Noncompliance Activity
6	Reconnaissance
7	Malicious Logic
8	Investigating
9	Explained Anomaly

Table 20: Event Categorization

2.4. Incident Response Model

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to manage the situation to limit damage and reduce recovery time and costs.

Although there are several variations in incident models, frameworks, and approaches, they all tend to follow six primary phases:

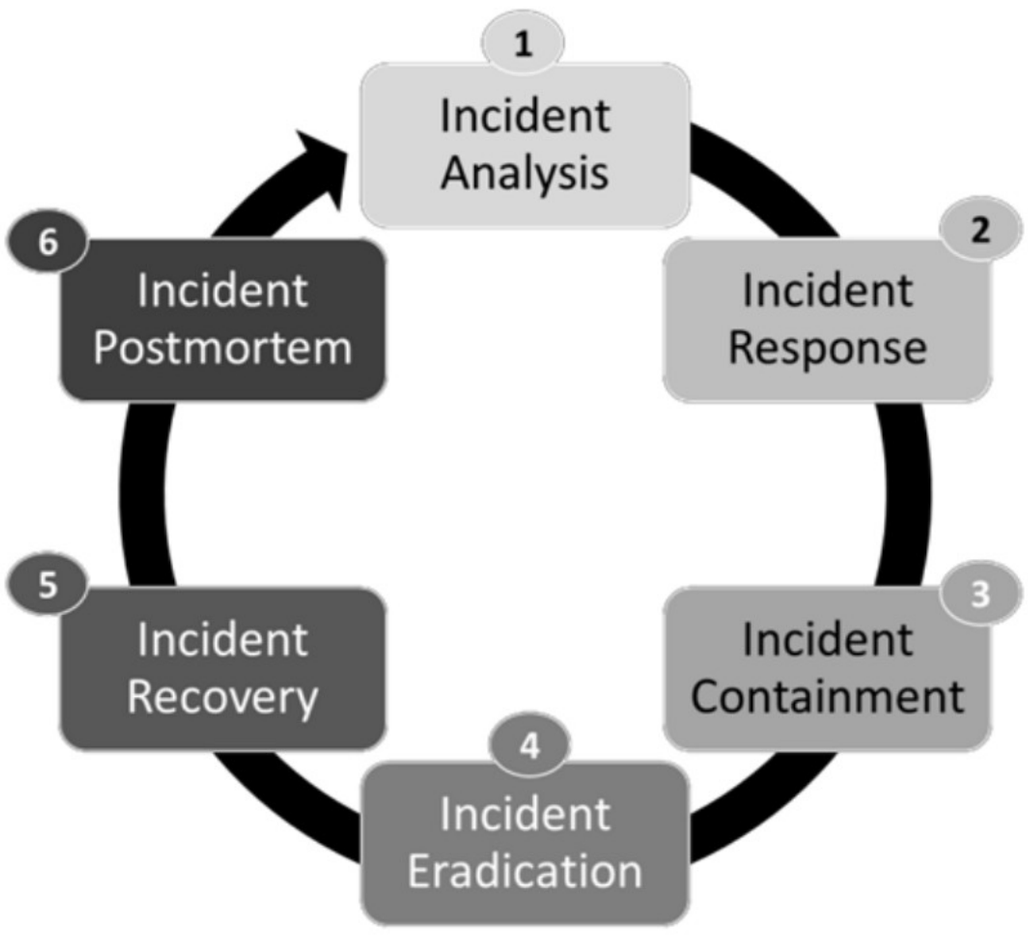


Figure 41: Incident Response Model

- **Phase 1 - Incident Analysis:** Incident analysis forms the basis of an organization's ability to respond effectively to computer security incidents. Computer security incidents are

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

often complex, multifaceted problems that require advanced analysis of technical details to understand what happened, find the root cause, and identify remediation steps necessary for recovery and response. The analysis requires experienced personnel to consolidate all the data points related to the incident. The correct data must be collected from suitable sources. Information provided during the initial analysis provides a roadmap for additional data-gathering efforts. Determining the root cause may lead one to identify weak or ineffective organizational controls.

The goal of the analysis is to identify the impact of an incident and identify appropriate escalation to support timely remediation. The impact will define the response priority for the incident within the context of other events and incidents the security operations team is managing.

- **Phase 2 - Incident Response:** The recovery procedures define the steps necessary to contain the incident, remove the threat, and restore operations. Incident response is complex. In practice, many activities co-occur as the organization works to respond appropriately to an event. The framework for incident response provides a consistent and repeatable approach to support the process. The framework presents phases in a logical, sequential order; however, active response often requires transitions back and forth between the phases as new information is discovered during the response process.
- **Phase 3 - Incident Containment:** Containment is concerned with limiting the extent of the attack/breach and potential losses. During this phase, the incident response team is activated to support the goal of isolating the issue and preventing the incident from spreading. Technical teams can work quickly to analyze the problem if they have previously profiled the systems to understand normal behaviors or if assistance is available from others who have experienced similar attacks. Evidence is preserved during this phase, which is essential for a response that leads to forensic investigation. Communications are also prepared to inform internal and external stakeholders.
- **Phase 4 - Incident Eradication:** This phase defines eliminating the cause of the incident. During this phase, the root cause of the attack is pursued beyond the initial investigation conducted during incident analysis. Affected hosts are identified, and the constituent components of the compromise are removed. The goal of eradication is to remove the cause of the incident altogether.
- **Phase 5 - Incident Recovery:** After the incident is contained and eradicated, the recovery phase defines the steps required to return the affected systems or services to their full normal state of operations. Three steps to ensure the return to normal operations in the recovery phase are as follows:
    - Determine the requirements for returning a system to service: This requires knowledge of system criticality and the exploit used in the compromise.
    - Prepare to reinstate the system: This may involve restoring systems from backups to ensure that files were not added to the environment for future unauthorized entry. It may include changing passwords, confirming configuration files have not changed, installing more patches, increasing the logging and monitoring capabilities, and improving the security by adding more controls or fine-tuning the operating security software.
    - Increase monitoring: Additional intrusion detection and prevention measures and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

increasing monitoring efforts will help ensure that the remediation steps are effective.

- **Phase 6 - Incident Postmortem:** Each new incident provides learning opportunities. Post-incident analysis offers an opportunity to evaluate the organization's event management and incident response procedures. New information gleaned from each recent incident should be part of every incident response process. A meeting after the event is addressed allows program staff to document root causes and lessons learned and revise strategies to support continuous improvement. The CISO should ensure that new information from each incident response activity is incorporated into the policy and procedures to improve the incident response process.

Developing Specific Incident Response Scenarios

Effective incident response plans provide specific response approaches to some of the most common incidents that could occur. Incident response plan scenarios typically evolve commensurate with the maturity of the plan. The following are some of the most common scenarios:

- **Insider Threat:** An insider threat is a malicious threat to an organization that comes from people, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.
- **Identity Theft:** Identity theft is the deliberate use of someone else's identity, usually to gain a financial advantage, obtain credit and other benefits in the other person's name, and to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, primarily if they are held responsible for the perpetrator's actions.
- **Mobile Device Loss or Theft:** Laptop and smartphone theft is a significant threat to users of laptop and netbook computers. Many methods have been developed to protect the data and prevent theft, including alarms, laptop locks, and visual deterrents like stickers or labels. Victims of laptop theft can lose hardware, software, and essential data that has not been backed up. Thieves also may have access to sensitive data and personal information. Some systems authorize access based on credentials stored on the laptop, including MAC addresses, web cookies, cryptographic keys, and stored passwords.
- **Phishing and Spear-phishing Attacks:** These types of social engineering attacks are often used to steal user data, including login credentials and credit card numbers. They occur when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. Phishing attacks can be broad, using basic techniques to fool many employees or very targeted (spear) against specific individuals.
- **Ransomware:** This type of malware restricts access to the infected computer system and demands that the user pay a ransom to the malware operators to remove the restriction.
- **Social Engineering:** It is a psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for information gathering, fraud, or system access, it differs from a traditional con in that it is often one of many steps in a more complex fraud scheme.

hideo1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2.5. Threat Management

Threat management begins by identifying and understanding the threats facing an organization. Threat actors can be natural or human, and their intentions can be accidental or deliberate. The CISO must understand these threats and their sources before developing a threat management strategy can begin. Once the threats are understood, the CISO must consider the likelihood of a threat overcoming weaknesses in a system, process, or environment to determine the impact. The conclusion of this process is an opportunity to rank and prioritize mitigation and controls to limit the impact of the identified threats.

The following is a threat management model:

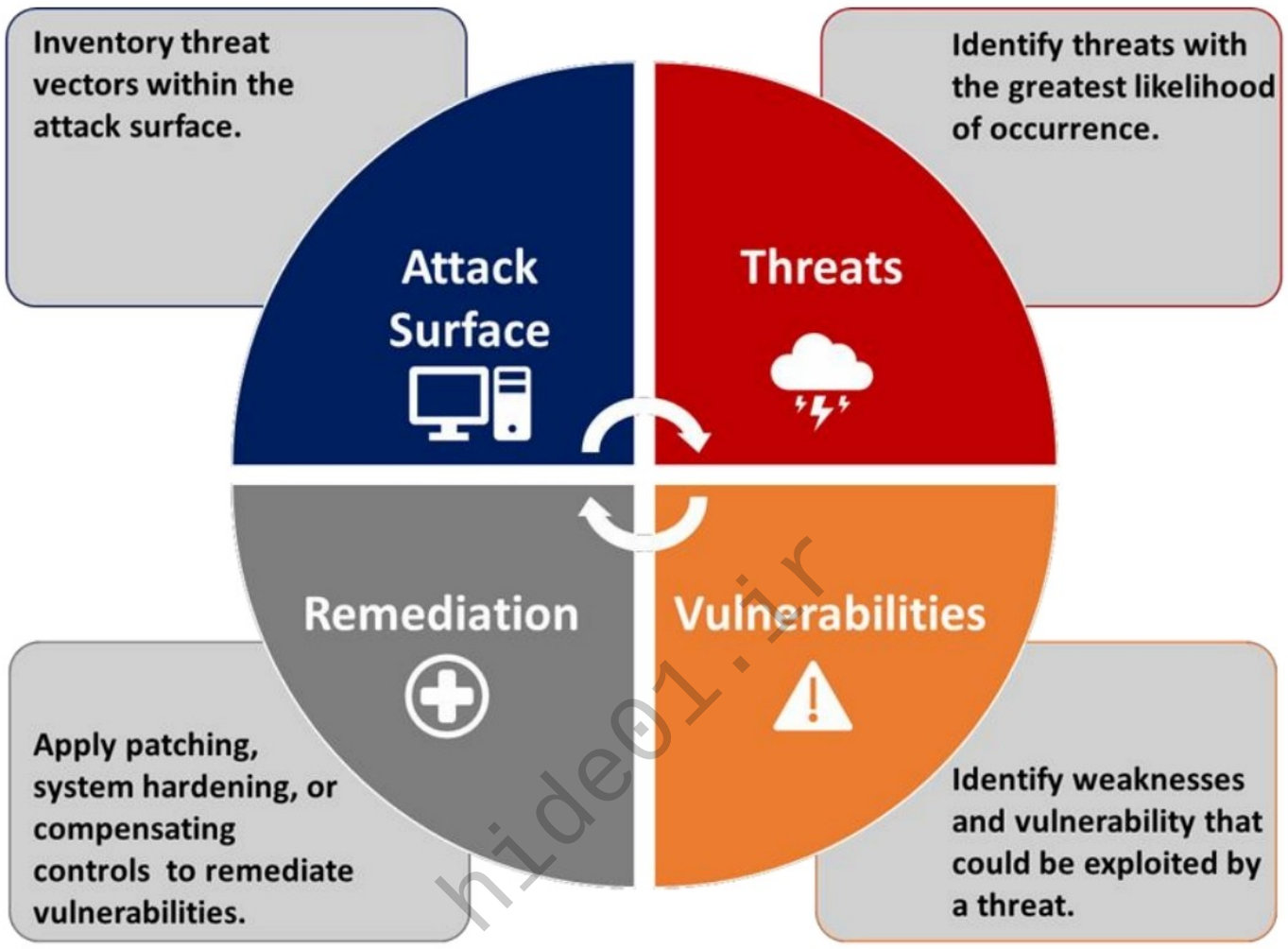


Figure 42: Threat Management Model

The following present the more common threat categories:

- **Outsider Threats**: Bad actors focus on the remote exploitation of systems to yield significant information and value to attackers. As technology advances, the number of attack vectors for technical threats increases. Therefore, the CISO is likely to devote the most time in the threat and vulnerability management program to identifying, understanding, and providing mitigation for the technical threats facing an organization.

A subset of the exhaustive list of technological threats follows:

- **Compromised Credentials:** Using another's identification can be a way to gain access and privileges to resources which the user is not entitled.
- **Exploitation of Software Vulnerabilities:** Software vulnerabilities are published through various sources and widely known. Any vulnerabilities that are left unpatched leave an organization vulnerable.
- **Malicious Software:** Trojan Horses, Rootkits, and malware meant to bypass other controls all provide access to information through a backdoor once the intruder has gained access.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Session Hijacking:** An unauthorized party can hijack an authorized session while maintaining the rights of the individual who established the session.
- **Insider Threats**: Insider threats include the intentional and unintentional activities conducted by employees to harm an organization. These acts range from data entry errors and inadvertent carelessness to intentional damage by disgruntled employees and espionage.
- **Physical Threats:** These are threats originating from nature and facilities. They range from utility failures like power and water to natural disasters like earthquakes and tornadoes. The physical and environmental controls discussed in Domain 4 address most of these threats. However, understanding the controls does not preclude the CISO from evaluating the likelihood and impact of valid physical and environmental threats facing an organization. These threats can destroy hardware and software assets and cause extensive damage to facilities and surrounding areas.
- **Social Engineering:** Social engineering leverages trust in relationships to trick a victim into disclosing information or authorizing activities that would otherwise be prevented. An attacker who uses social engineering effectively is playing on the weaknesses of human nature, either the inherent desire to be helpful or the intrinsic curiosity of people. Attackers can use digital or physical means to accomplish their goals. The physical means can use voice or face-to-face interactions. In contrast, digital attacks use pop-up windows, phishing, and drive-by downloads to trick victims into divulging information or installing malicious software that facilitates additional compromises.

2.6. Threat Intelligence

hide01.ir

Organizations ready to move to the next level of threat management can turn to external intelligence services to aid in their threat decision-making process. Actionable intelligence is critical to guiding threat management investments. Dedicating personnel to scour the internet looking for threat intelligence or gleaning threat data from Information Sharing and Analysis Center (ISAC) alerts has proven ineffective. The alternative is to outsource threat intelligence gathering to companies sourcing threat information.

For over 20 years, companies have offered threat intelligence services to help organizations stay ahead of the threat curve. Early services relied on manually sifting through vendor vulnerability reports. Now, intelligence services are faster, more in-depth, and highly targeted toward advanced persistent threats. Today's services have solved this industry's relevance problem for some time. Now, only threat information aligned to an organization's attack surface or industry makes it to the CISO's desk.

- **Honeynets and Honeypots:** Faux IT infrastructure with decoy information to attract hackers to waste their time on the wrong targets.
- **Information Sharing and Analysis Center (ISAC):** Commercial critical infrastructure section threat intelligence shared by specific industries.
- **Open-Source Intelligence (OSINT) Feeds:** Intelligence collected from publicly available sources.
- **Security Information and Event Management (SIEM):** Security event log collection, aggregation, and analysis to detect malicious activity.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Threat Intelligence Subscriptions:** Commercial subscription to threat intelligence gathering and reporting services.

Requirements guide the gathering of threat intelligence and its analysis to make it actionable. The following are things to consider when documenting requirements for threat intelligence:

- Track bad actors targeting your organization.
- Acquire threat information aligned to your attack surface.
- Know which hacktivist organization targets your industry and
- Understand the techniques adversaries use to exploit vulnerabilities in your enterprise.

2.6.1. Information Sharing and Analysis Centers (ISAC) [81]

Information Sharing and Analysis Centers (ISACs) are nonprofit organizations that provide a central resource for gathering information on cyber threats (in many cases critical infrastructure) and allow two-way information sharing between the private and the public sectors. ISACs have created communities within the private sector. They could be oriented on a specific critical industry (for example, finance, energy or health) or serve as a focal point on the national level to gather information about cyber incidents and analyze them. ISACs were created in the United States in 1997. After the first terrorist attacks on the World Trade Center (1993) and Oklahoma City (1995), President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP).

Its objective was to identify the possibility of cooperation between the public and private sectors so that U.S. critical infrastructure could be adequately protected. Chaired by Robert T. Marsh, the commission presented the so-called Marsh Report [82] with many recommendations for raising the level of critical infrastructure in the United States. One of the main recommendations was to establish Information Sharing and Analysis Centers (ISACs) to build and strengthen cooperation between public administration and industry. Today, 23 sector-based ISACs comprise the National Council of ISACs (NCI) in the United States. Formed in 2003, NCI collects and analyzes cyber and physical threat intelligence, sharing this vital information with member companies in their sectors. ISACs have the cooperation of the public sector—the Department of Homeland Security, where the U.S. Computer Emergency Readiness Team (CERT) is located. Some of them are also active in Europe [81] (for example, financial service (FS) – ISAC).

2.7. Vulnerability Management

Vulnerabilities represent weaknesses that can be exploited to gain unauthorized access to information. Vulnerabilities can apply to physical as well as logical aspects of security. The vulnerability management strategy developed by the CISO should reduce the likelihood that threat actors can exploit vulnerabilities that exist in the organization.

The CISO should ensure that vulnerabilities are identified across all organization platforms. Vulnerabilities require prioritization according to importance and potential impact. Note that a vulnerability does not necessarily cause harm by itself. The motivations and capabilities of the attack influence the likelihood associated with the exploitation of a vulnerability. For example, existing application errors in software create a vulnerability for an organization. Still, an attacker must know about the vulnerability and the means to exploit it before an organization can evaluate the impact of the vulnerability. In addition, mitigation of vulnerabilities on systems with limited

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

business impact would be prioritized lower than those with a higher business impact.

All vulnerabilities should be addressed eventually. In aggregate, an attack that exploits numerous low vulnerabilities could have the same impact on the organization as a single attack that exploits a moderate or a high vulnerability.

The three common approaches to support the vulnerability management program are vulnerability assessments, penetration testing and patch management.

2.7.1. Vulnerability Assessments

Vulnerability assessments are typically tool-based approaches using scanners to identify weaknesses in a system. Findings from the assessments can be used to help develop a remediation strategy that addresses the vulnerabilities before threat actors can discover and exploit them.

Vulnerability scanners are critical in identifying potential security weaknesses within an organization's systems. These scanners rely on extensive databases of known vulnerabilities to detect misconfigurations or software susceptibilities that attackers may exploit. It is essential to regularly update these vulnerability repositories to ensure that the latest threat intelligence is incorporated, enabling a more accurate assessment of system vulnerabilities. This update process is vital for prioritizing which vulnerabilities pose the most significant risk to the organization.

Network scanners, on the other hand, focus on scrutinizing network environments. They pinpoint open ports, poorly configured services, and operating system and software weaknesses. By identifying potential attack paths and points of exploitation, network scanners help organizations prioritize their defensive efforts.

hide01.ir

Host scanners, similar in functionality to network scanners, often operate within a narrower scope. They assess individual hosts or devices for vulnerabilities and misconfigurations. Understanding each host's attack path and potential exploitability is crucial for efficient mitigation.

Once these scanning tools identify vulnerabilities and deficiencies, technical personnel must evaluate them to determine their relevance and severity. Prioritization is critical in this process, ensuring that resources are allocated to address the most pressing security concerns first. Some scanning tools offer built-in criticality ratings based on predefined criteria from vendors, providing an initial level of prioritization. However, manual evaluation remains essential to discern valid or irrelevant findings from false positives.

In addition to assigning numerical or qualitative risk ratings, some tools enable organizations to conduct trend analyses of vulnerabilities over time. This capability assists security teams in understanding the evolving threat landscape and adapting their security measures accordingly. Overall, effectively prioritizing vulnerabilities, considering their exploitability and potential attack paths, is paramount to crafting a robust and initiative-taking cybersecurity strategy.

Vulnerability scanning can be performed periodically or as part of a defined schedule. Vulnerability scanning analysts should understand security controls within the environment, use a current asset inventory, and review prior assessments. Vulnerabilities should be tracked until remediation is complete. The risk management program typically accounts for this.

Scans can be credentialed or noncredentialed. Credentialed scans are preferred because they provide more accurate vulnerability data. They allow the scanning tool to perform a more

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

thorough check, looking for problems that cannot be seen from the network. Noncredential scans probe the target from the network and only identify exposed vulnerabilities.

2.7.2. Vulnerability Management in Practice

Vulnerability management programs vary across organizations; however, a relationship exists between the vulnerability management program's effectiveness and the program's maturity.

The vulnerability management program should strive to improve maturity by addressing the following:

- Organizational policies must define the vulnerability management program and the expectations of the program. Policies define behavior and expectations. Clear expectations are critical for success.
- Organizational executives must buy into and endorse the program. Vulnerability management can create disruptions in business processes. Executive support is critical to remove barriers and avoid conflicts.
- Mature asset management is critical. The organization knows who owns assets that may be affected by the vulnerability management program so that they can participate in the program activities.
- Mature change management is critical. A mature change management program must exist to support scheduled and expedited remediation of vulnerabilities in organizational systems and processes.
- The maturity of the organization's project and program management practices influences vulnerability management's effectiveness, which is complex and requires effective coordination to achieve a successful outcome.

2.7.3. Penetration Testing

Penetration testing attempts to access resources without knowledge of usernames, passwords, and other normal means of access. Penetration tests discover information system flaws that vulnerability scans and assessments might not identify. Periodic penetration tests are a good practice to discover information system flaws not identified by vulnerability assessments or patch management practices [83]. They may identify meaningful findings beyond the scope of system vulnerabilities.

Penetration testing can occur through external tests conducted by a third party or as internal tests. There are multiple testing methodologies used to probe an environment for vulnerabilities. Each approach has its merits and may be combined with other tests. The tests provide perspective about an attacker's ability to exploit vulnerabilities in the organization. Because of the potential to disrupt operations or obtain unintended access to restricted or confidential information, testing should be performed with the full support of organizational leaders and the consent obtained before executing the test.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following describes the various types of penetration testing:

Black Box Testing	White Box Testing
• Testers have little to no prior knowledge of the systems or environment before performing testing. • Testers must use the same techniques as hackers. • Most rigorous of all penetration testing techniques	• Testers have substantial knowledge of the systems and environment before performing testing. • Potentially more vulnerabilities are exposed due to the methodical nature of the test. • No inhibitors to performing detailed system analysis of target applications.
Gray Box Testing	**Crowd Sourced Testing**
▪ Testers have limited knowledge of some or all of the systems and environment before performing test. ▪ Combination of black and white testing techniques used	• Testers are professional hackers with substantial experience penetrating systems. • Testers can be selected based on expertise in compromising specific systems and environments.

Figure 43: Penetration Testing Options

hine01.ir

2.7.4. Security Testing Teams

With a tradition stemming from military training exercises, many institutions have taken up the idea of pitting a Red Team of trained attackers against a Blue Team defending the organization over the years.

The following shows the interrelationship within the security testing teams:

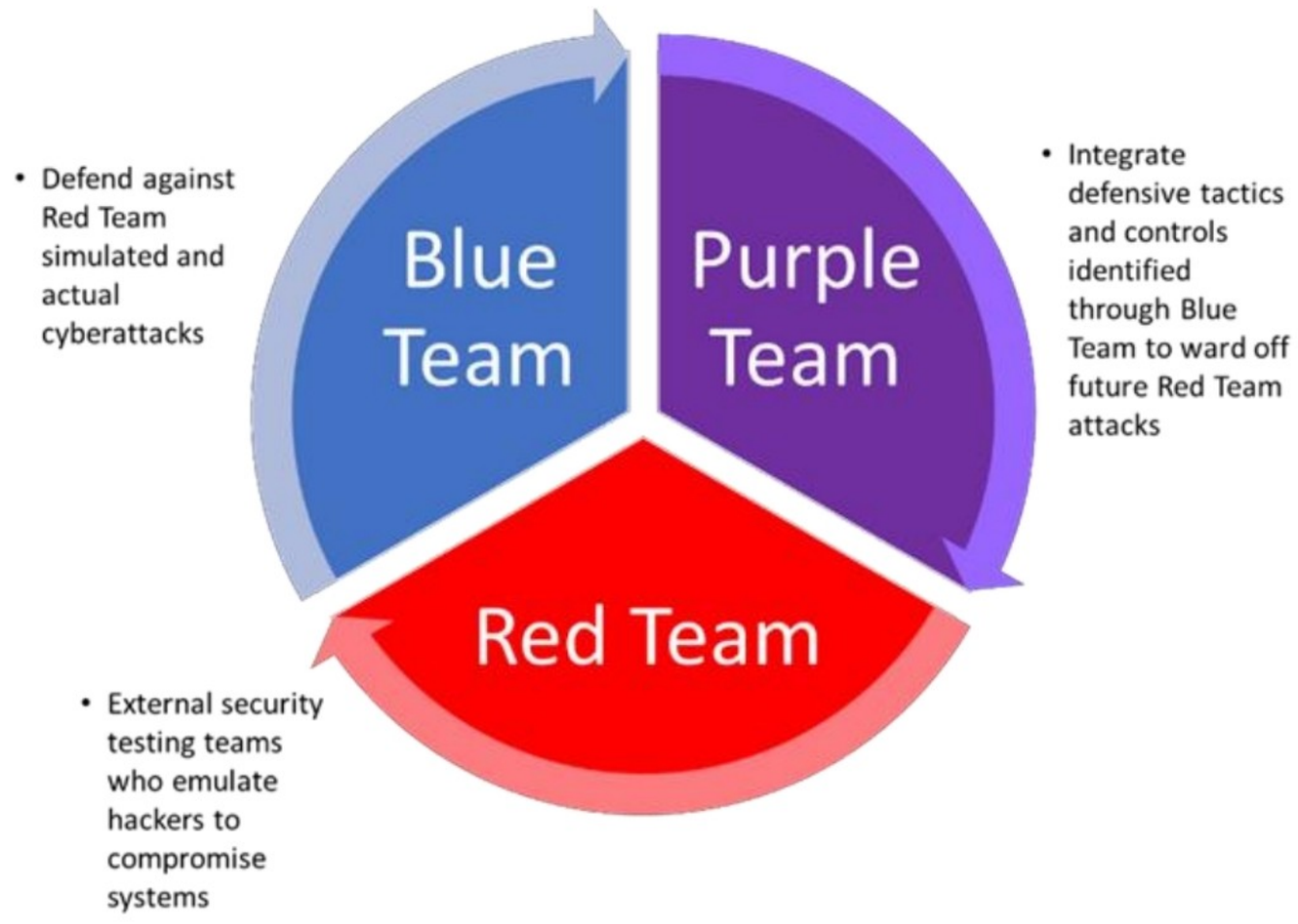


Figure 44: Testing Team Interrelationship Model

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Red Teams:** Red Teams are external entities brought in to assess the effectiveness of an organization's security program rigorously. They emulate the tactics, techniques, and procedures of potential attackers to uncover vulnerabilities and weaknesses in the security posture. While some Red Team engagements have specific objectives, others focus on comprehensive security evaluations. The insights gained help organizations enhance their overall security readiness.
- **Blue Teams:** Blue Teams represent the internal security teams tasked with defending against real-world threats, including external attackers and Red Teams. They aim to maintain vigilance against potential threats, monitor network activity, respond to incidents, and improve defensive measures. Blue Teams are pivotal in safeguarding an organization's assets and data.
- **Purple Teams:** Purple Teams serve as collaborative units bridging the gap between Red and Blue. Their primary goal is to maximize the effectiveness of both offensive and defensive security efforts. Purple Teams achieve this by integrating the findings from Red Team assessments with the defensive strategies and controls employed by the Blue Team. This collaborative approach ensures that vulnerabilities identified by the Red Team are promptly addressed and that security measures are optimized for real-world protection.

The primary goal of a Red Team is to identify opportunities for enhancing the Blue Team's capabilities. Consequently, in organizations where the collaboration between the Red Team and Blue Team is operating effectively, the necessity for Purple Teams should be minimized or even eliminated.

r-tde01.ir

2.7.5. Remediation

Patch management is a complex activity that requires coordination throughout the organization. The CISO and the information security program must work with IT, change management, and business stakeholders to support the patch management strategy. Patches address hardware and software vulnerabilities but can also add new features. An effective patch management program must coordinate efforts to ensure outcomes achieve the expected results.

Guidelines for Enterprise Patch Management [47]

The National Institute of Standards and Technology's Guide to Enterprise Patch Management Planning (NIST SP 800-40) defines patch management as identifying, acquiring, installing, and verifying patches for products and systems to correct security and functionality problems in software and firmware. Organizations should implement the following recommendations to improve the effectiveness and efficiency of their enterprise patch management technologies:

- Organizations should deploy patch management tools using a phased approach.
- Organizations should reduce the risks associated with enterprise patch management tools by applying standard security techniques when deploying an enterprise-wide application.
- Organizations should balance their security needs with their needs for usability and availability.

Timing, prioritization, and testing are critical aspects of effective patch management, with

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

numerous security companies reporting that many attacks are preventable with appropriate patch management.

An organization must create a system patching schedule before implementing patches and document objectives and activities in formal policies and procedures. This ensures consistency in the program.

Patch installation timing should align with regular maintenance windows or use unique schedules for critical categories of patches. For example, applying critical patches is the highest priority and is done as soon as practicable. More time is typically provided to evaluate and install patches categorized as low or moderate.

The schedule should also provide adequate time for testing patches. As a patch management component, the organization should establish a testing environment to evaluate the impact of patches on systems before installing patches. Patches change the way a system or software operates. Understanding the influence of those changes in the testing environment is essential rather than potentially experiencing downtime because a patch created an unintended production system interruption.

2.7.6. System Hardening:

System hardening is the application of security configurations, software, or other protections. Operating systems like Windows, UNIX, Linux, iOS, and Android are typically configured to run on a least functionality principle. This ensures that only services needed to provide the required functionality are available.

Because software operating systems contain millions of lines of code and introduce complexity in development and testing, errors are prone. This allows vulnerabilities to be present, and exploits can be developed after the software is released.

Services, permissions, ports, protocols, and remote connection services are defined as part of the standard configuration and are applied during the baseline process. Also, unnecessary ports and protocols are removed to prevent unauthorized device connections.

2.7.7. Database Hardening:

Most of the critical information in an organization is stored in a database. Effective security hardening of databases is essential to reduce vulnerabilities and improve risk status. Database operating systems function similarly to server and endpoint operating systems. Therefore, the tools, techniques, and processes used to achieve system hardening, in general, often apply to hardening and protecting database systems.

Database hardening is not limited to the server on which the database resides. The database security strategy should ensure that applications accessing the database are also evaluated for the effectiveness of their security controls.

2.8. Threat Hunting

Threat hunting provides tactics, techniques, and procedures to validate existing threat detection strategies used by the security operations program. The activities conducted by the threat-hunting team also identify opportunities to enhance tuning for automated tools to improve their discovery of valid events not already being detected. Whereas event management and incident response are reactive, threat hunting is an initiative-taking approach to enhance the effectiveness of the security operations program.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacker Hunting: Mission, Strategy, and Tactics [84]

Hunting's primary value is its ability to uncover new patterns of behavior related to an attack and tune existing security tools to identify the behavior more effectively. Different hunting activities exist depending on their purpose and the data available to support the hunt:

- **Exploratory Hunt:** The hunter develops and explores attack scenarios. For example, a vulnerability in a web application has been exploited to upload malware into a production environment.
- **Structured Hunt:** The hunter evaluates the information in existing security tools for signs of anomalous activity. Such a scenario might be the discovery of an unauthorized endpoint conducting transmission control protocol (TCP) scans in a production subnet.
- **Guided Hunt:** The hunter processes data from multiple tools and sources to identify indicators of compromise that have been overlooked or assigned low-priority ratings by automated systems. A blocked Domain Name System (DNS) query goes to a known malware domain; the antivirus console identifies several attempts to turn off the antivirus software on a host, or network behavior analysis notices that a Transmission Control Protocol (TCP) scan has been run from that host.

None of the data points, taken individually, would generate an alarm or trigger an event management and incident response. However, in aggregate, the data points indicate the possibility of an undetected compromise on the host and additional efforts to facilitate lateral movement within the network. At this point, the incident should be referred to the incident response team for validation and further action.

The four phases of the Threat Hunting Loop represent an iterative process supporting the defined approach. Each phase produces information that can be used to start new hunts and to provide intelligence on existing threats. Once a cycle has been completed, the processes involved in that hunt can be automated and added to existing incident response processes.

The following is a model of a threat-hunting loop developed by Sqqrl (Amazon):

Figure 45: Sqrrl (Amazon) Threat Hunting Loop

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. SUMMARY

Domain 3 covered the role of a CISO as a program manager and the skills and resources required to design and implement an effective information security program. It also highlighted the importance of sponsors and stakeholders and how to effectively communicate with them to build program integrity and transparency. Developing and executing a strategic plan as a playbook creates consistency in information security service delivery.

Managing the finances of an information security program will call on new skills, subsequently requiring CISOs to understand financial management and basic accounting concepts. Building a relationship with the organization's CFO and likely a core sponsor of the information security program is essential to program funding.

Planning for the backup and recovery of critical operations is another role CISOs play today. It is increasingly common for security and continuity pillars to blend where similar skill sets and resources can be leveraged, and economies of scale may be achieved. Cloud-based recovery and security services are gaining popularity, and CISOs should evaluate the benefits of moving some information security program services to the cloud.

The designated security leader will spearhead the incident response efforts in a security incident. This includes the collection of digital evidence, ensuring its integrity, and maintaining a secure chain of custody, primarily if the evidence might be utilized in legal proceedings.

Overseeing the security operations portion, where threats and vulnerabilities are identified and defended, is one of the most essential functions of an information security program. CISOs must also know how to attack their organizations through red teaming and penetration testing.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.
hide01.ir

C|CISO

hide01.ir

DOMAIN 4

Information Security Core Competencies

EC-Council

Introduction

To function effectively, gain the respect of your subordinates, and apply information security correctly, a CISO must have a solid foundation in the core technologies used to protect information and assets. CISOs can find it challenging to keep up with the latest technologies and keep pace with the myriad responsibilities of running an IS program. CISOs from a technical background will want to attempt to do it all and be as technically savvy as their staff. CISOs who try to do the role of manager and technician need to do both roles properly.

As your organization's IS program head, you must be a thought leader in identifying key cybersecurity technology. Still, you do not have to know the intricacies or how to operate all the technologies. This domain will introduce you to the core competencies to protect your organization's attack surface. This includes the endpoints to the network and everything in between.

Knowledge Assumptions

It is assumed that you already have a working knowledge of primary information technology commonly found in an enterprise. For example, we expect that at this level, you understand the function of routers, the operating principles of a data center, and the basic lifecycle of application development. This domain will serve as either a refresher or fill in the blanks of your knowledge set. At the least, it connects how IS interrelates to technology.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. ACCESS CONTROL

Unauthorized access is one of the most critical concerns addressed by CISOs today. Security control weaknesses or deficiencies can lead to policy violations and security incidents when poorly managed. The 2021 Open Web Application Security Project (OWASP) lists A01:2021-Broken Access Control as the most severe web application security risk [61]. This study highlights the importance of managing access control effectively within an organization.

1.1. Authentication, Authorization, and Auditing

You were likely introduced to the triple-A access control model early in your career. Authentication, authorization, and auditing (AAA) is a long-lived model for articulating controlling access to computer resources, enforcing access policies, and auditing user activity. Regardless of the solutions deployed for each "A" of the model, the concept remains constant.

Each "A" of the model is explained below:

- **Authentication:** The act of confirming the authenticity of an attribute of a single piece of data claimed valid by an entity. For our purposes, an entity is a person whose identity must be confirmed before access can be granted to assets or resources.
- **Authorization:** Specifying access rights to assets and resources is required once an identity has been confirmed. Here, users have privileges, such as the permissions they should be granted to assets, resources, and(or) data. This is the principal component of an access control policy.
- **Auditing:** Once validated users have authorized access to assets and resources, monitoring and reporting on how they use what they have been granted access to is essential. This is done through logging of user access to systems and applications.

hide01.ir

The third "A" in the model is sometimes referred to within a cloud-computing context as accounting, where the resources consumed by a user are accounted for and billed.

The following is a logical representation of the AAA model:

Figure 46: AAA Model

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.2. Authentication

Authentication defines the process used by a system to verify the identity of a user, process, or service before granting access. Unique identification is vital for successful access control. Data sensitivity and the confidence required to verify the identity of a remote user influence the authentication strategy and the number of factors used to support access to remote systems. The critical aspects are the authentication processes and the methods used to identify individuals.

- **Electronic authentication model:** Electronic authentication, or e-authentication, establishes confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet; however, in some cases, access to the network may be limited, and access control decisions may take this into account.

  E-authentication begins with registration, which provides an opportunity to verify the registrant's identity. Authentication establishes confidence in the registrant's identity rather than addressing authorization or access privileges. When approved, the system owner uses a registrant's identity to make access control decisions once the process is complete.

- **Authenticator management:** Involves the processes and procedures for issuing and revoking authenticators used in the access control process. Authenticators include passwords, tokens, biometrics, public key infrastructure (PKI) certificates, and key cards [85]. Device authenticators may consist of certificates and passwords. Ensuring authenticators are distributed securely and that processes exist for managing lost or damaged authenticators is critical.

  The authenticator management process should be applied to hardware and software products. In many cases, information system components are shipped with default authentication credentials. This allows rapid and simplified initial installation and configuration; however, they must be changed after installation activities are completed. Default authentication credentials are often well-known, easily discoverable, and present a significant security risk [85].

- **Authentication approaches:** The risk posed by compromised credentials emphasizes the importance of authentication and the need for effective authentication processes. The CISO should understand the benefits and risks of each potential approach and select the best option that supports the needs and priorities of the organization.

- **Single-factor authentication:** Maps an authenticator (usually a password) to an account to facilitate authentication. Account credentials grant access to resources with all the rights, privileges, and access associated with that account. The simple username and password combination is inexpensive, and implementation is simple. The negative aspect of this approach is that it results in the weakest form of authentication control for an organization.

  Some organizations attempt to address known weaknesses of the single-factor approach by increasing the length and complexity requirements for passwords. This increases entropy, which reduces predictability and the potential to determine a user's password.

  Even with these controls, human factors limit the effectiveness of single-factor authentication. Users often reuse corporate passwords for authentication on social

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

networking platforms and other places with weaker controls. Users often select passwords that are easy to remember and may be easy to determine using standard password-cracking techniques.

- **Multi-factor authentication:** Maps two or more attributes to an account to facilitate access. This strategy combines something you have, something you know, or something you are, in the authentication process. This increases the likelihood that the system can accurately confirm the identity of a user requesting access and make an appropriate access decision. For example, physical tokens that combine a one-time password with a personal identification number (PIN) increase confidence in the user's identity. An attacker is unlikely to have the token and know the PIN chosen for the token.

  CISOs can increase or decrease authentication factors based on the confidence about the user's identity required for system access. Systems that require moderate confidence may only require single-factor authentication. Systems that demand more confidence may require two or more factors. Adding factors increases the cost and the complexity of the authentication solution. Therefore, CISOs must balance the solution's benefits with the organization's needs to ensure the solution fits the environment.

- **Passwordless authentication,** also known as certificate-based authentication, uses a public/private key pair to confirm the authenticity of an identity. This does not rely on any knowledge-based factors like passwords. Instead, biometric signatures are often (but not always) used during the authentication flow. Standard methods include fingerprints, retinal or iris scans, and facial and voice recognition. The FIDO Alliance aims to reduce the world's over-reliance on passwords using these biometric factors alongside Trusted Platform Modules (TPM), USB tokens, smart cards, and near-field communications (NFC). The FIDO2 Project expands these methods to the web and applications with Web Authentication (WebAuthN) and Passkeys. These methods are resilient to phishing-based attacks and are considered the logical successor to single-factor authentication. The CISO should consider the cost and complexity this introduces before adopting it in a large enterprise environment.

- **Identity management:** The CISO is responsible for ensuring effective identity management because of the influence this activity has on the organization's access control strategy. Authentication of an individual's identity is a fundamental component of physical and logical access control processes because an accurate determination of an individual's identity is needed to make sound access control decisions. Identity management defines the technique used to recognize individuals accurately before granting access to an organization's systems, facilities, and resources.

Many factors influence the extent to which the organization verifies the identity of individuals. The CISO should ensure an identity management solution is selected that supports the sensitivity of the information that must be accessed. The strategy must consider both the cost and the structure of the organization. The centralized or distributed nature of the organization also influences the process. Decentralized organizations may require dedicated resources in each locality to support identity verification.

CISOs can leverage existing organizational processes to improve identity management. HR, for example, collects significant data and may perform background checks supporting identity verification. Additionally, HR can be the primary means to determine an identity's status and track its lifecycle. For example, when an employee's identity is disabled due to separation. Similarly,

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CISOs in organizations with a mature vendor management process can leverage information from that process to support the identity verification of vendors and contractors working with the organization.

CISOs can increase or decrease authentication factors based on the confidence required for system access. Systems that require moderate confidence may only require single-factor authentication. Systems that demand more confidence about the user's identity may require two or more factors. Adding factors increases the cost and the complexity of the authentication solution. Therefore, CISOs must balance the solution's benefits with the organization's needs to ensure the solution fits the environment.

1.3. Authorization

Authorization defines granting a user or object permission to perform or obtain something. This concept describes the systems that can be accessed and what can be done once access is granted. The CISO's role in authorization includes defining policies, processes, and procedures regarding access requirements. These are typically based on principles of least privilege, need-to-know, and separation of duties. The CISO can implement additional controls and mitigation strategies to support enforcing authorization principles defined by the organization. This may include monitoring unsuccessful sign-ins, enabling notifications of system use, and identifying last sign-in or concurrent sessions.

- **Least privilege principle:** The least privilege principle states that individuals or systems should only have the access necessary to perform specific activities required for their job or role. Certain roles, such as systems administrator or database administrator, require higher privileged access. An administrative assistant on the other hand, would have a different level of access. If the same level of access was provided to all individuals, the risk increases due to the potential for errors, improper information access, or the increased ability to commit fraud.

  Security processes such as changing the firewall-filtering rules or creating access should be explicitly assigned by using privileged accounts. These activities should only be performed by specified personnel or groups.

  When individuals are not performing work on these activities, they should not use the privileged access accounts. The principle of least privilege is sometimes referred to as minimally necessary access. The access is provided according to the minimum amount of information required to perform the task. The principle of least privilege ensures that what can be done with the data (read, change, delete, or execute) is limited to the least amount of access necessary to perform those actions.

- **Need-to-know principle:** Access to systems should only be granted to individuals with a legitimate need to know the information within those systems. For example, a nurse may only need to see the information on an individual's medical record for a patient he/she is assisting. The nurse does not need access to the records of all patients at the hospital. Highly classified information may also require elevated security clearances in order to access the information. A manager may need to know the salary of personnel on their team but does not need to know salary information for other departments. These are all examples of the need-to-know principle.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.4. Auditing

Auditing when a user accesses assets and resources is essential to compliance and security reporting. CISOs can never assume authenticated and authorized users will always behave or use information and/or systems correctly. Insider threats are a genuine concern and a growing risk. To that end, a CISO must have auditing practices in place to track and report on user activity. Create an audit policy to ensure auditing of user activity that makes sense and not simply create abnormally large log files. Referencing that policy, auditing was required to understand who accessed what and when.

The following outlines the minimum level of user account auditing required:

- Failed access attempts to restricted information or sensitive administrative operations.
  - Anomalous administrative operations include creating, reading, updating, or deleting (CRUD Security Matrix). Examples include users logging on in more than one location simultaneously.
- Detected sign-ins while users are on vacation, sick leave, etc.
- Validation of access appropriate for job responsibilities.
- Access to information outside of the job role.
- Suspicious patterns of access.
- Suspicious time and/or day(s) of access.

The frequency of audit reviews will determine whether it is the sole means to uncover inappropriate access. A security information event management (SIEM) solution can alert on these audit conditions as they occur.

hideen.ir

1.5. User Access Control Restrictions

Users can be instrumental in reporting or preventing potential system abuse, provided they have the right tools to assist them. Access control systems can be deployed to provide the following:

- **Last sign-in notification:** Notifying the end user of the previous sign-in can provide information to the end user to determine if unauthorized access was obtained using their account. The end user can then act by following the incident reporting process.
- **Unsuccessful sign-ins:** Limiting the number of unsuccessful sign-in attempts by a user during a specific period can reduce the potential for guessing credentials. Procedures may include locking accounts after a certain number of attempts, requiring an end user to contact the help desk, or simply unlocking the account after a specified period of time. A typical mobile device control erases information on the mobile device if a certain number of incorrect sign-ins have been attempted.
- **Concurrent sessions:** A situation that occurs when two or more sessions exist simultaneously. This may be prohibited because most users only create a single session for system access. Additional sessions using the same credentials might indicate malicious behavior or a compromised account. The exception may be system administrators; however, this can be serviced by issuing multiple credentials to perform their varied activities.
- **Time-based access:** Limiting sensitive administrative access for a brief period. This

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

typically aligns with an approved change window or emergency access. Once the change window is closed, the access is promptly removed. This reduces the attack surface since elevated permissions are not kept permanent. This practice works well with an Identity Governance Administration (IGA) tool.

1.6. User Access Behavior Management

Influencing behavior through restrictions and awareness is part of a comprehensive approach to access control. Two behavior management techniques include:

- **Separation of duties:** Separation of duties divides the responsibilities associated with an action or process to decrease the opportunity for misbehavior or policy violations through collusion. As more individuals become involved in a process, it becomes less likely that all parties will agree to the malicious or inappropriate action. For example, personnel implementing controls should refrain from auditing the controls for effectiveness. A negative incentive exists for the implementer to evaluate effectiveness. Using an independent evaluator increases the likelihood that the audit will result in an evaluation representative of the actual state of the control.
- **Notification of system use:** Banners are sign-in displays that notify the user they are accessing a confidential system, and if they access this system, they may be subject to monitoring, audits, etc. Notices often include the right to pursue criminal prosecution or impart civil penalties if the individual is not authorized to access the system or if they inappropriately use it. Users are requested to accept these conditions before gaining access. CISOs must collaborate with their general counsel or legal departments to ensure the message is worded correctly.

1.7. Types of Access Control Models

At the highest level, identity management systems typically comprise three significant elements: users, applications, and policies. Policies define how the users interact with the different systems and applications, which are subsequently enforced by access control methods.

Four primary types of access controls are used to define or enhance the strategy within an access control plan.

- **Discretionary access control:** Discretionary access control (DAC) permits the user to decide how to protect the information and level of sharing. Access to files is restricted to users and groups based on their identity and the groups to which the users belong.

  The access policy protecting information objects may allow users to change security attributes or grant access to other users. For example, if a user created a file, that user would retain the right to be able to read, update, or delete the file. The user may grant access to other users to read the file but may restrict others from deleting it. These controls are discretionary because the end user can establish and maintain the level of access by other individuals.

- **Mandatory access control:** Mandatory access control (MAC) does not permit users to pass privileges onto other users. Instead, access control is managed centrally to define the extent to which actors can perform predefined activities on an object.

  MAC customarily functions at the operating system level to govern computer threads and processes' actions on objects. MAC also provides increased control for managing user

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

access to critical or high-priority systems. MAC is used to ensure that only authorized individuals can access systems or data based on data classification levels rather than the role of the user requesting access.

- **Role-based access control:** Role-based access control (RBAC) assigns access privileges based on the allowed actions of the user and is independent of the user's identity. This strategy requires a clear definition of roles within an organization and the access permissions associated with each role. A role is assigned to a user, and the user's access is limited to the rights and permissions assigned to that role. As a user takes on multiple roles, access increases according to the combination of all assigned roles.

  Role-based access can simplify the privilege assignment, ensuring that individuals have only the privileges necessary to perform their duties based on the roles associated with their job(s). The organization must accurately determine the access required by each function and decide on the number and types of roles that should be supported.

- **Attribute-based access control:** Attribute-based access control (ABAC) is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of the entity's (subject and object) actions and the environment relevant to a request. Attributes may be considered characteristics of anything defined and to which a value may be assigned. In its most basic form, ABAC relies upon evaluating attributes of the subject, features of the object, environment conditions, and a formal relationship or access control rule defining the allowable operations for subject–object attribute and environment condition combinations.

The following table presents the four most common access control models:

Discretionary Access Control (DAC)	Mandatory Access Control (MAC)	Role-based Access Control (RBAC)	Attribute-based Access Control (ABAC)
This model allows an individual complete control over any objects they own along with the programs associated with those objects	This model gives only the owner and custodian management of the access controls. This means the end user has no control over any settings that provide any privileges to anyone	This model provides access control based on the position or responsibility an individual fill within an organization	This model relies on rules or policies that define allowable operations of how users can access or use information and resources

h1t601.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Discretionary Access Control (DAC)	Mandatory Access Control (MAC)	Role-based Access Control (RBAC)	Attribute-based Access Control (ABAC)
Least restrictive model popular in situations where resource owners need to allow access and privileges on demand (SharePoint)	Most restrictive model typically used in defense or military organizations where data classification and confidentiality are of prime importance	Flexible model for large organizations desiring to implement least privilege and segregation of duties. Popular in heavily regulated organizations or companies with high turnover	Most flexible and detailed of all access control types. Access can be granted by IP address, time, dates, resources, objects, privileges, or any combination thereof

Table 21: Access Control Type Comparison

1.8. Designing an Access Control Plan

An access control plan outlines the organizational strategy for access control. The plan defines the procedures and details required for achieving the objectives described in the organization's access control policy. Developing an access control plan helps the CISO formalize the approach for managing access to IT environments or facilities. Formalizing the strategy and documenting a plan equips the CISO to collaborate with business leaders and identify unique access control objectives required for individual business processes and activities. This approach also helps avoid security deficiencies when organizations limit their access control policy or fail to meet the requirements defined in a regulation or compliance framework.

Customizing an access control plan to address the unique concerns of an organization requires consideration of the following:

- What are the access control goals and objectives of the organization?
- What risks will the access control strategy remediate?
- What account types and security groups are required to support this strategy?
- What is the authentication, authorization, and access administration strategy, including provisioning and decommissioning access?
- What is the process for recertifying access for authorized users?
- What unique security policies are required for remote access, system accounts, and system connections?
- What is the relationship between the access control plan and other security controls?

1.9. Access Administration

Access administration involves the processes and procedures needed to manage access of a user or object, from provisioning to decommissioning or termination.

- **Access provisioning (provision):** Access administration establishes the account for a user or object, provides only the access required, and is typically based on documented procedures. HR is a critical partner in the process of access administration. Most often,

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

initiating access procedures begins during initial employment as part of the new-hire process or onboarding. The organization should define prerequisites for granting access and provisioning credentials, including requirements for screening and proving individual identity.

Some organizations prohibit system access provisioning for new employees until background screening and initial security training are complete. The organization should document and retain provisioning information for historical purposes and to support audit processes. For example, information related to access provisioning may be required for a data discovery request or audit to determine whether a user had access to a system at a given time.

- **Access monitoring (review):** Monitoring access changes allows for determining if users still need access. It is imperative to monitor administrators' elevated access to databases, security technologies, and networking infrastructure because of the potential damage that could result from abusing these privileges. Reviews of these accounts and associated privileges should occur regularly.

  During the transfer of employees to other roles, physical and logical access should be reviewed to ensure that the access is provided as needed by the individual. Keys, badges to buildings, offices, or access to a different business unit area may no longer be required. Transferred employees often get little attention, as managers are reluctant to remove access because:

- They may only know the real access needs for the position if the system is set up based on roles.
- They are afraid of inadvertently removing a capability required for the job.

Physical and logical access needs to be rechecked with every organizational transfer.

- **Access termination (remove):** The access administration process should define procedures to remove access as part of the termination process for personnel. This should be integrated with the change management or disposition process for system access.

Employee terminations require prompt removal of logical and physical access. Terminations correctly managed by the manager, human resources representative, and physical security reduce the risk of security violations. While most terminations are not volatile if appropriately managed, physical security must be aware and available during an adverse event.

The following is a representation of the access administration lifecycle:

Figure 47: Access Administration Lifecycle

hideo1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. PHYSICAL SECURITY

Physical security protects personnel and assets from events and circumstances that could cause severe loss or damage to an organization. Physical controls protect an organization's interests and assets and are as important as logical controls within IT systems.

Physical security is often overlooked, and its importance should be considered instead of focusing on technical security. An attacker can conduct physical security breaches with little or no technical knowledge. Accidents and natural disasters are also a part of the physical security threat model.

2.1. Designing, Implementing, and Managing a Physical Security Program

Although CISOs are not involved in physical security and facility design, they are frequently asked to provide insight into where the program may be leveraged or intersect with material design. The closer the facility is to technology, for example, a data center, the more involvement a CISO will have.

2.1.1. Physical Risk Assessment

Once the physical risk analysis is complete, the organization can develop a physical security strategy. One strategy manages physical security as three distinct actions: obstacles and prevention, surveillance and notification, and response and recovery.

Physical security must balance the need for control with the need to operate the business. The principles of information risk management are similar to physical risk management. The value of assets, the perceived susceptibility to various threats, and the potential impact of these threats exploiting weaknesses will determine risk profiles for physical assets and help identify controls. This determines the number of resources an organization is willing to use to protect physical assets.

hideel.ir

Risk management for physical threats and vulnerabilities follows the same process used to evaluate digital/cyber risks. The time to implement controls, ease of use, and influence on business processes and operations should be considered when assessing controls that address an organization's physical risks.

When valuing physical assets, care must be taken to consider the value of the information regarding the asset. A tablet or laptop may only cost a few hundred dollars; however, if the device is lost or stolen, its information may be worth much more than the device itself. It could contain business strategies, intellectual property, customer records, sensitive identifiers, network designs, or financial information worth much more than the equipment.

2.2. Physical Location Considerations

- **Geographic location:** The physical location is critical. A facility may be improperly located in an area having an elevated risk of terrorist attack, such as near a tall landmark or in a space where large numbers of people may be present (for example, a football stadium). The location may also be prone to natural disasters such as tornadoes, hurricanes, forest fires, or floods. If the building is in a high crime area, it may be subject to more frequent break-ins and susceptible to theft. Locating a data center near train tracks could increase the risk of an explosive fuel train car accident.
- **Multi-tenancy:** Organizations often occupy offices in a building shared with other tenants. Physical access control may be more difficult when sharing resources with other

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

tenants in the facility. Telecommunications may also be using shared infrastructure, requiring logical separation of circuits. Shared data centers may require isolated cages to restrict access.

- **Building materials:** The construction of a building will contribute to the overall security of the facility. Walls for secured rooms should go floor to ceiling and not be accessible via the ceiling tiles. Steel doors provide more protection than glass or wood doors. Windows should be evaluated for placement and replaced with walls (if not needed). This is particularly true for the ground level floors. Windows should incorporate alarm systems, and the glass's or other material's strength should be evaluated for adequate protection.

2.3. Obstacles and Prevention

Physical security strategy focuses on physical barriers and shelters protecting facilities from physical attack or limiting the impact of natural disasters.

Protection from physical attackers is achieved by using a strategy of layered defense. The layers create an increasingly complex set of obstacles an attacker must overcome to conduct a successful attack or compromise. The edge of the physical perimeter should include gates and checkpoints to manage traffic flow into and out of facilities. The entryways for the facility should provide additional layers of protection to control traffic, which includes protected entrances, mantraps, or human security guards. Within the facility, restricted and unrestricted areas should be segregated.

Areas requiring higher levels of protection may include server rooms, file areas, telecommunications closets, data centers, and others to which only a limited number of people should have access.

hide01.ir

Protection from accidents is achieved by implementing physical and environmental controls that mitigate the outcome of fires, floods, and power interruptions. Many control catalogs guide implementing physical and environmental controls that help protect systems and personnel. For example, the National Institute of Science and Technology (NIST) SP 800-53 R5 [49] includes a family of controls dedicated to physical and environmental protection.

- PE-1: *Physical and environmental protection policy and procedures* require consideration for controls that facilitate the implementation of physical and environmental protection controls.
- PE-9: *Power equipment and cabling* require consideration for protecting power equipment and cabling from damage or destruction.
- PE-11: *Emergency power* requires consideration for short-term uninterruptible power supplies to facilitate orderly shutdown of systems.
- PE-13: *Fire protection* requires consideration for fire suppression and detection systems.
- PE-15: *Water damage protection* requires consideration for protecting systems from damage resulting from water leakage by primary shutoff and isolation valves.

Protection requirements for environmental disasters are difficult to determine; however, organizations can plan to mitigate environmental disasters' impact on facilities and personnel. Many of these considerations are addressed as part of business continuity planning and management. Also, organizations can design facilities to resist the effects of disasters or incorporate controls (such as shelters and reinforcement) within a facility to protect personnel and essential equipment.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Barriers to entry:** Various entry controls may be needed, such as continuous barriers around the property of a manufacturing plant. Fencing is the most used physical protection, and various types exist. Concrete barriers may be installed to manage the risk of vehicles entering sites or high-volume human traffic areas.
- **Lighting:** Facilities should be well-lit to function as a deterrent. Auxiliary sources of power to maintain a lower lighting level during a power outage will help facilitate orderly evacuation or return to normal operations.
- **Door locks:** Locks come in many styles, from key or combination locks to proximity badge readers. Deadbolt locks have a bar that goes into the doorframe. Locks provide elevated levels of security, but they require keys that can be easily duplicated. Locks rarely change when personnel leave the organization, creating a potential security risk. Hotels have mitigated key risks by using magnetic-strip keycards for room entry. If metal keys are used, access to the primary keys must be tightly controlled and accessible to a limited number of individuals. Combination locks can provide a less expensive alternative, as they permit the access code change.

Proximity cards are challenging to duplicate and provide more control for restricting access. Some systems combine logical systems access and physical access within the same card. Some companies place their logo on the keycard so that if it is lost or stolen, it may be returned.

2.4. Secure Facility Design

CISOs are generally not involved directly with the secure design of a building except for when the IS program converges with the life/safety aspects of the facility. The critical characteristics of facility design that CISOs do, as a matter of course, become involved in include, choosing locations for data centers, SOCs, SCIFs, and other technology-centric spaces. The following summarizes secure area designs CISOs will likely be involved in.

2.4.1. Security Operations Center

In this instance, a Security Operations Center (SOC) is defined as a facility dedicated to and organized to prevent, detect, assess, and respond to cybersecurity threats and incidents and fulfill and assess regulatory compliance. Building a SOC - or creating some form of internal security operations capabilities - is a costly and time-consuming effort that requires ongoing attention to be effective. Indeed, many organizations (including some large organizations) choose not to have a SOC and instead engage a managed security service provider (MSSP).

Below are the various SOC approaches:

- **In-house SOC (I-SOC):** In-house SOCs are dedicated SOCs where the organization provides all the facilities, tools, services, and personnel to monitor and respond to cyber and internal threats against organizational assets.
- **Hybrid SOC (H-SOC):** This is a hybrid approach where an organization outsources some services of their SOC operations or contracts for non-prime time coverage.
- **Managed services SOC (M-SOC):** Outsourced implementation of a SOC where most SOC operations are contracted to an MSSP. Organizations still retain the accountability of the SOC regardless of the outsourced relationship.
- **Security Network Operations Center (SNOC):** An implementation approach where the network operations center (NOC) is combined with the functions of a

chideo1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SOC. In this approach, NOC and SOC personnel share facilities, responsibilities, and tools.

- **Virtual SOC (V-SOC):** Virtual implementations of a SOC do not rely on a centralized or dedicated facility. Personnel used to staff the positions of a V-SOC tend to be part-time or provided through staff augmentation contracts. Much of the SOC activity is automated, and the SOC focuses on reacting to critical events.

CISOs and technology leaders contemplating building their own SOC should know this approach's cost and staffing implications.

2.4.2. Sensitive Compartmented Information Facility

The U.S. Department of Defense created the concept of sensitive compartmented information facilities (SCIFs) to define a secure area that had appropriate protections in place to ensure to the greatest extent possible that the extremely sensitive information inside would not be compromised. SCIFs have specific requirements when it comes to construction, particularly in terms of physical security, visual controls, acoustic controls, access controls, and electronic and TEMPEST security.

These requirements are outlined in a U.S. government document called Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities - Version 1.5.1 - IC Tech Spec - for ICD/ICS 705 – July 26, 2021 [86].

2.4.3. Digital Forensics Lab

Designing and building a forensic laboratory is a complicated undertaking. It requires a high degree of planning and performance standards to ensure integrity. Digital evidence is often collected for submission in a court of law. A poorly designed lab decreases the likelihood of evidence maintaining its integrity. Exacting requirements for cleanliness, temperature, humidity, and vibration controls are necessary to create an environment suitable for forensic science.

To assist in this process, the NIST Interagency/Internal Report (NISTIR) - 7941 - Forensic Science Laboratories: Handbook for Facility Planning, Design, Construction, and Relocation [87] is available. This handbook is a resource for laboratory directors, designers, consultants, and other stakeholders involved in the construction or significant renovation of forensic science laboratories. Laboratory construction and renovation projects must meet the unique needs and requirements of the regional law enforcement and criminal justice community it serves. This document guides forensic laboratory facility planners on how to meet these requirements by applying principles, processes, tools, and resources applicable across a broad range of facility types. This document strives to highlight basic facility lifecycle processes as well as those specific requirements that are unique to forensic science laboratories.

2.4.4. Data Center

Data center security refers to all the precautionary measures defined in the standards for data center infrastructures to secure the data center from natural or human disasters. The Uptime Institute began rating classes of data centers in 1993 and has published four tiers of data centers based on resiliency:

nidoo1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

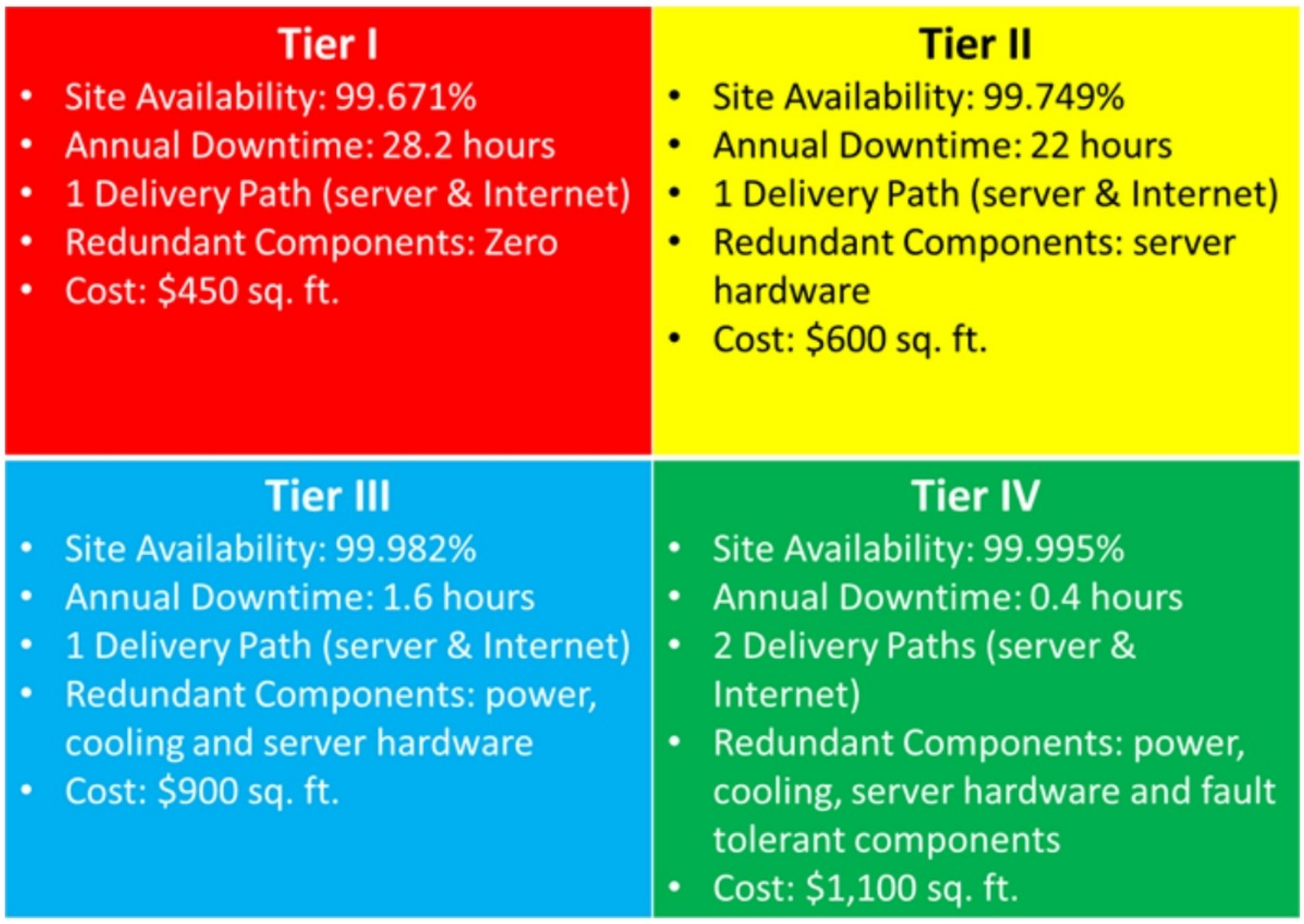


Figure 48: Uptime Institute Data Center Tier Classifications

The following is a high-level summary of the design considerations required of a data center.

- **Security**
  - *Site selection*: Data centers should be in low-risk areas that are least subjected to natural threats (flooding, hurricanes, earthquakes, and so on) and manufactured risks (airports, highways, construction density, and so on).
  - *Physical security*: The data center should not be advertised, all entrances for loading and guests should be monitored, and access should be controlled. Perimeter fencing, bollards, and other deterrents should be in place.
  - Site monitoring: All access points and areas where damage could occur require 24/7 closed circuit television (CCTV) monitoring.
- **Resiliency**
  - *Construction: The data center should be designed to withstand the most common natural threats. The facility should withstand 200 mph winds and have specialized roof membranes or waterproofing to resist driven rain.*
  - *Utilities: Multiple utility providers should be available for electrical, fiber, and water.*
  - *Mechanical: Provide dual cooling and heating appropriate to the heating and cooling needs of the equipment.*
  - *Fire protection: Data centers and all support equipment rooms require FM 200 or pre-action sprinkler systems commensurate with local and national fire codes. Early smoke detection apparatus (VESDA) should be used to address a fire proactively.*
  - *Leak sensing*: Sensing devices should be placed near all water sources and points of potential water leakage.

h1de01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2.5. Preparing for Physical Security Audits

Audits should be performed regularly to ensure the selected physical security controls are implemented and working as intended. Corrective action must occur to address any audit findings that identify physical control weaknesses.

Social engineering could be used by someone trying to enter a facility without the appropriate credentials, typically by posing as an employee. For example, holding controlled entry doors open for others is usually prohibited. This could be evaluated by modeling the behavior and performing physical access testing.

CCTV systems can be evaluated by walking through areas and determining if coverage is adequate. A CISO can conduct periodic assessments of digital recordings to confirm that data is retrievable. Doorjambs can be evaluated for forced entry; alarms can be assessed if installed.

3. NETWORK SECURITY

The CISO must ensure that the policies and procedures exist to support security for an organization's network communications. The CISO does not manage routers and configure network technology but must be aware of the technologies used to support network communication, and the impact technologies have on information security controls and services. This requires a mature understanding of device interactions and the security impact of network configurations. Knowledge of the network architecture also helps to understand where the information flows are and the security policies, procedures, and controls needed to protect it.

hide01.ir

3.1. Network Security Assessments and Planning

Enterprises divide technology, network, and security management responsibility between various roles. The CISO often focuses exclusively on risk management and other security-centric activities, while the CIO or CTO leads efforts for network planning. The network planning process is essential to help an organization achieve its information security goals so the CISO and/or their information security team should be involved.

Network Security Checklist [88]

The following items support an effective network security plan:

- Focus on value rather than return on investment. Consider the harm a network security breach could do to the organization, such as lost revenue or customer litigation.
- Never assume security issues will originate only from outsiders. Employees can accidentally create security vulnerabilities, and disgruntled or former employees can cause considerable damage.
- Refrain from addressing security issues with a piecemeal approach; use a single, unified strategy that protects the whole network.
- Collaborate within the organization to develop and implement security strategies, focusing on technology, training, and physical site security.
- Find the right balance between security and usability. The more secure the network is, the more difficult it can be to operate effectively.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3.2. Network Security Architecture Challenges

The CISO is rarely responsible for network management in an organization; however, many network management concerns influence decisions made about network security within the organization. The fundamental problems are network discovery, the influence of multi-tiered architectures, the risk of a single point of failure in the networking environment, and network address translation (NAT) for routing traffic within the network.

The following lists are some of the challenges CISOs face when working with network management to create a secure network environment:

- Defining ownership, responsibility, and accountability of security devices (firewalls and IDS/intrusion prevention systems [IPSs]) connected to the network.
- Balancing network hardening with disabling functionality and throttling throughput.
- Agreeing on network security devices and technologies.
- Defining a shared security responsibility model for networked devices.
- Defining budget for network investments that includes security capabilities.

3.3. Network Security Design

CISOs must work closely with network architects to create a security design that protects the organization's information and assets. Breaking down the process of security design into the following steps will assist with effective collaboration on a network security strategy:

hide01.ir

- Identify network assets.
- Analyze network security risks.
- Analyze network security requirements and tradeoffs.
- Develop a security plan.
- Define a network security policy.
- Develop procedures for applying network security policies.
- Develop a technical implementation strategy.
- Achieve buy-in from users, managers, and technical staff.
- Train users, managers, and technical staff.
- Implement the technical strategy and network security procedures.
- Evaluate the network security and update it if any problems are found.
- Maintain network security state.

3.4. Network Standards, Protocols, and Controls

3.4.1. Network Security Standards

ISO/IEC 27033 is a multipart standard derived from the existing five-part International Organization for Standardization (ISO)/IEC 18028. The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation, and use of information system networks and their interconnections.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CISOs should be able to adapt the material in this standard to meet their network security requirements.

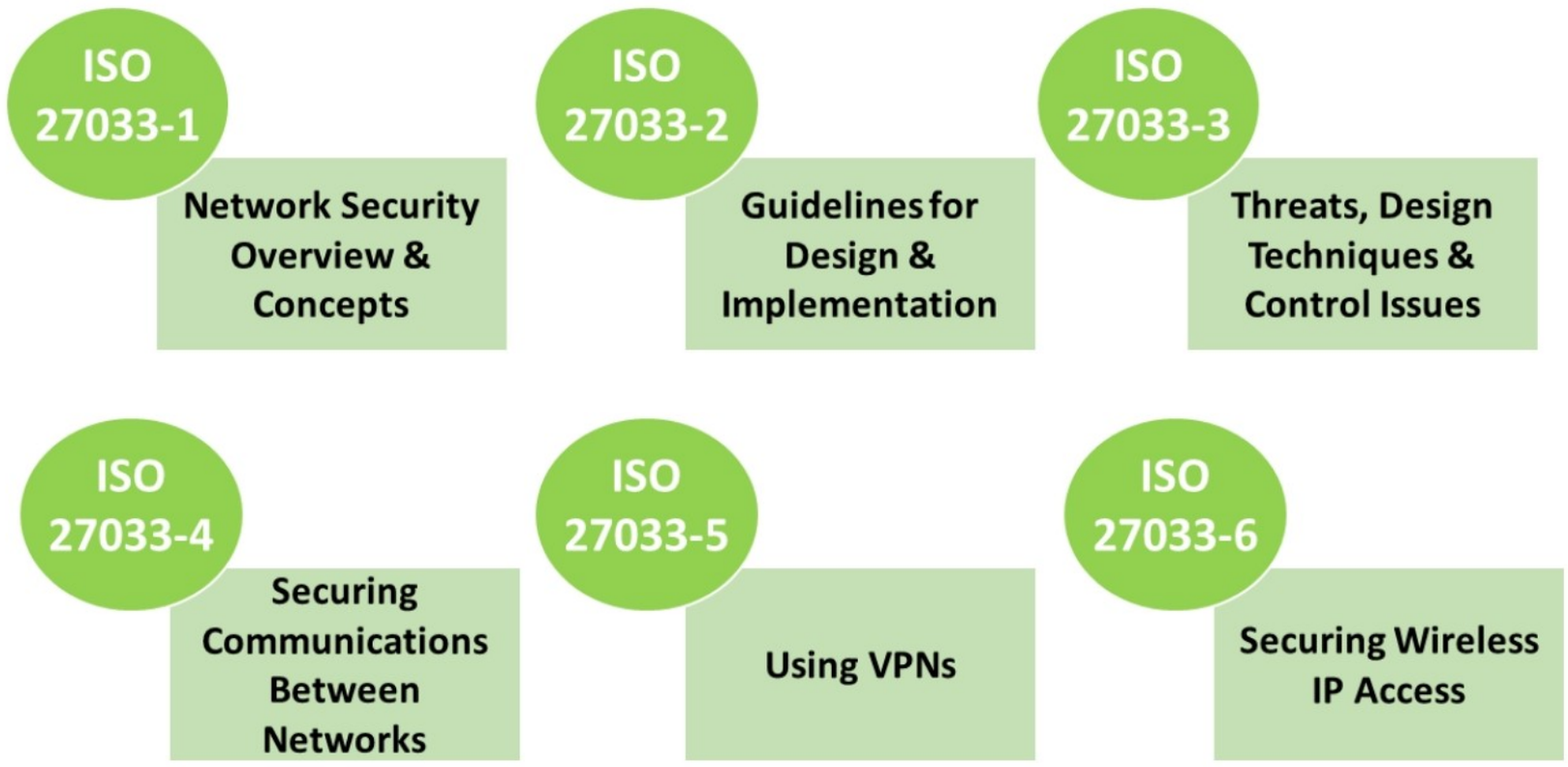


Figure 49: ISO Network Security Standards

ISO/IEC 27033 provides detailed guidance on implementing the network security controls introduced in ISO/IEC 27002. It applies to the security of networked devices and the management of their safety, network applications/services, and network users, as well as to the protection of information being transferred through communications links. It is aimed at network security architects, designers, managers, and officers.

ISO/IEC 27033-1:2015 | Network security overview and concepts [88]

Defines and describes the associated concepts and provides management guidance on network security. This includes providing an overview of network security and related definitions and advice on identifying and analyzing network security risks and defining network security requirements. It also introduces how to achieve superior quality technical security architectures and the threat, design, and control aspects associated with typical network scenarios and network "technology" areas (dealt with in detail in subsequent parts of ISO/IEC 27033).

ISO/IEC 27033-2:2012 | Guidelines for the design and implementation of network security [89]

Defines how organizations should achieve quality network technical security architectures, designs, and implementations that will ensure network security appropriate to their business environments, using a consistent approach to the planning, structure, and implementation of network security, as relevant, aided by the use of models/frameworks (in this context, a model/framework is used to outline a representation or description showing the structure and high-level workings of a type of technical security architecture/design) and is relevant to all personnel who are involved in the planning, design, and implementation of the architectural aspects of network security (for example, network architects and designers, network managers, and network security officers).

ISO/IEC 27033-3:2010 | Reference networking scenarios—threats, design techniques, and control issues [90]

Defines the specific risks, design techniques, and control issues associated with typical network

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

scenarios. It is relevant to all personnel who participate in the planning, designing, and implementing the architectural aspects of network security (for example, network architects and designers, network managers, and network security officers).

ISO/IEC 27033-4:2014 | Securing communications between networks using security gateways [91]

Defines the specific risks, design techniques, and control issues for securing information flows between networks using security gateways. It is relevant to all personnel who participate in the detailed planning, design, and implementation of security gateways (for example, network architects and designers, network managers, and network security officers).

ISO/IEC 27033-5:2013 | Securing communications across networks using virtual private networks [92]

Defines the specific risks, design techniques, and control issues for securing connections that are established using virtual private networks (VPNs). It is relevant to all personnel who participate in the detailed planning, design, and implementation of VPN security (for example, network architects and designers, network managers, and network security officers).

ISO/IEC 27033-6:2016 | Securing wireless IP network access [93]

Defines the specific risks, design techniques, and control issues for securing Internet Protocol (IP) wireless networks. It is relevant to all personnel who participate in the detailed planning, design, and implementation of security for wireless networks (for example, network architects and designers, network managers, and network security officers).

hide01.ir

3.4.2. Protocols

A network protocol defines rules and conventions for how networks communicate. Network protocols provide the means for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgment and data compression designed for dependable, high-performance network communication.

The following describes more likely protocols CISOs will experience:

Internet Protocols

The IP family contains a set of related (and among the most widely used) network protocols. Besides IP itself, higher level protocols like:

- **File transfer protocol:** The file transfer protocol (FTP) is a standard network protocol that transfers computer files between a client and server on a computer network. FTP is built on a client–server model architecture and uses separate control and data connections between the client and the server.
- **Hypertext transfer protocol:** An application protocol for distributed, collaborative, and hypermedia information systems. Hypertext transfer protocol (HTTP) is the foundation of data communication for the web.
- **Transmission control protocol:** One of the main protocols of the IP suite. It originated in the initial network implementation, complementing the IP.
- **User datagram protocol**: It is a part of the IP suite used by programs running on different computers on a network. User datagram protocol (UDP) is used to send

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

short messages called datagrams, but overall, it is an unreliable, connectionless protocol.

The above protocols integrate with IP to provide additional capabilities. Similarly, lower-level IPs like address resolution protocol and Internet control message protocol also coexist with IP. Generally, higher-level protocols in the IP family interact more closely with applications like web browsers, while lower-level protocols interact with network adapters and other computer hardware.

Wireless Network Protocols

Wireless networks have become commonplace thanks to Wi-Fi, Bluetooth, and long-term evolution (LTE). Network protocols designed for wireless networks must support roaming mobile devices and deal with variable data rates and network security issues.

Standard Wi-Fi protocols include:

- **Bluetooth**: Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices and building personal area networks.
- **LTE**: LTE is a standard for high-speed wireless communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface and core network improvements.

Network Routing Protocols

Routing protocols are special-purpose protocols explicitly designed for use by network routers on the Internet. A routing protocol can identify other routers, manage the pathways (called *routes*) between sources and destinations of network messages, and make dynamic routing decisions.

Standard routing protocols include:

- **Border gateway protocol (BGP)**: A standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (ASs) on the Internet. The protocol is often classified as a path vector protocol but is sometimes called a distance-vector routing protocol.
- **Enhanced interior gateway routing protocol (EIGRP)**: An advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration.
- **Open shortest path first (OSPF)**: A routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols operating within a single autonomous system (AS).

Modern operating systems contain built-in software services that implement support for some network protocols. Applications like web browsers include software libraries that support the high-level protocols necessary for that application to function. For some lower-level transmission control protocols and Internet Protocols (TCP)/(IP) and routing protocols, direct hardware (silicon chipset) support is implemented for improved performance.

Each packet transmitted and received over a network contains binary data (ones and zeros that encode the contents of each message). Most protocols add a small header at the beginning

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of each packet to store information about the message's sender and intended destination. Some protocols also add a footer at the end. Each network protocol can identify messages of its kind and process the headers and footers as part of moving data among devices.

A group of network protocols that work together at higher and lower levels is often called a protocol family. Students of networking traditionally learn about the Open System Interconnect (OSI) model that conceptually organizes network protocol families into specific layers for teaching purposes.

OSI Model

The CISO should be familiar with the seven layers of the OSI model, and the activities or operations performed at each layer. The ISO published the OSI model to facilitate network communication.

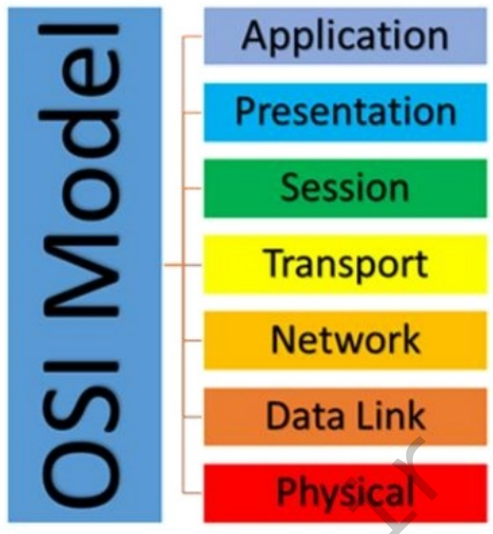


Figure 50: OSI Model

The seven-layer framework model indicates which networking standards can be developed for which layer of the model.

- **Layer 1: Physical layer**: The physical layer includes the cabling, networking hardware, and network adapter cards, ensuring that electrical signals are distributed to the intended nodes on the network. At this layer, the topologies of bus, star, ring, and mesh are implemented.
- **Layer 2: Data-link layer**: The data-link layer provides the means to form and distribute packets across the network. This layer listens to determine when to send the packets and how to process collisions or route packets. Switches and bridges operate at this layer. This layer uses media access control (MAC) addresses assigned to each device to route the information from the higher layers and provide data integrity.
- **Layer 3: Network layer**: The network layer routes messages between the computers using logical addressing, whereby addresses are assigned to devices used by the network protocols, such as IP or IPX. Routers operate at this level and deliver packets utilizing a routing table indicating the next hop on the network. Internet protocol security (IPsec) works at the network layer to authenticate the hosts and provide encryption capability. It is also often used to create VPNs to permit gateways to tunnel through the Internet instead of through expensive point-to-point connections.
- **Layer 4: Transport layer**: This layer ensures that the packets are received without errors and in the correct order. As the lower layers send packets, they might be received in a different order than they are sent. TCP reassembles the packets into a message. TCP is called a connection-oriented protocol, whereas UDP is connectionless because

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

it does not try to ensure the packets are assembled in an order.

- **Layer 5: Session layer**: The session layer provides the mechanism for opening, closing and managing a session between end user application processes, e.g., a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications. Session-layer services are commonly used in application environments that make use of remote procedure calls (RPCs).
- **Layer 6: Presentation layer**: The presentation layer indicates how the information will be available to the receiving computer. This layer may determine that the data will be presented using the American Standard Code for Information Interchange (ASCII) format, the most familiar format for text files on computers and on the Internet. Encryption and compression might also be used at this layer.
- **Layer 7: Application layer**: This layer provides the interface for applications to communicate with the network. Several protocols operate at this layer, such as domain name system (DNS) to resolve Internet domain names, FTP for file transfers, and simple mail transfer protocol (SMTP) to support email operations. Security protocols, such as secure shell protocol (SSH), are implemented at the application layer for encrypted command line sessions for remote sign-in over the Internet. Secure HTTP operates at the application layer to protect web traffic.

The following is a view of the OSI model mapped to countermeasures:

OSI Model Layers		ISO 7498-2 Security Model	Example Countermeasures
7. Application	Logical – Software Oriented	Authentication	• Directory security • Email security • Host firewall • Secure browser • Secure coding • Secure file transfer protocol (FTP) • Secure printing
6. Presentation		Access Control	• Data encryption • Identity and access management (IDAM) • Message encryption • Secure coding
5. Session		Non-Repudiation	• Message nonrepudiation • Password encryption • Remote login security • Session expiration • Token management
4. Transport		Data Integrity	• Firewalls • Port restriction • Session Security
3. Network	Physical – Hardware Oriented	Confidentiality	• Access control list (ACL) • Firewalls • IPsec • Network intrusion detection system (NIDS) • Malicious packet inspection • Network routing protection • Secure domain name service (DNS)
2. Data Link		Assurance/Availability	• Firewalls • Media address control (MAC address) filtering • Wireless security
1. Physical		Notarization/Signature	• Biometric authentication • Data storage encryption • Electromagnetic shielding

hide01.ir

Table 22: OSI Model Mapped to Countermeasures

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3.4.3. Network Security Controls

The CISO must understand the standard controls and approaches for protecting network communications. To increase the effectiveness of these controls, the organization must define policies and procedures for the related technologies in advance. Also, the organization should ensure that network security solutions are appropriately tuned to achieve intended outcomes and results.

The following are the must-have network security technologies to defend against today's threats:

Boundary Protection

Monitoring and control of communications at the external boundary or perimeter of an information system to prevent and detect malicious and other unauthorized communication using boundary protection devices (for example, proxies, gateways, routers, firewalls, guards, encrypted tunnels).

- **Firewall (external)**: A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, which is assumed not to be safe or not trusted. It separates networks with differing security requirements.
- **Edge routers**: Edge routers accept inbound traffic into the network. These edge devices characterize and secure IP traffic from other edge routers and core routers. To ensure security, edge routers can either be configured with tools that include access control lists or purchased with built-in firewall support. This enables more advanced security safeguards, including VPN tunnels and signature matching through intrusion prevention and detection technologies (IPS/IDS).
- **Network Address Translation (NAT)**: The more an attacker knows the configuration of a network, the easier it is to get to an information source. NAT works to hide the internal network addresses from external entities through a process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. Firewall rule restrictions are also used to limit probes to gather information regarding the organization of an internal network. The primary use of NAT is to limit the number of public IP addresses an organization or company must use for both economic and security purposes, and it allows for stricter control of access to resources on both sides of the firewall.
- **Network intrusion detection system (NIDS)**: A network-based intrusion detection system monitors and analyzes network traffic to protect a system from network-based threats. A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered based on severity, the system can act, such as notifying administrators or barring the source IP address from accessing the network.
- **Secure web gateway (SWG)**: A secure web gateway is primarily used to monitor and prevent malicious traffic and data from entering or even leaving an organization's network. Typically, it is implemented to secure an organization against threats from the Internet, websites, and other Web 2.0 products/services.
- **Security group (cloud environments)**: A security group controls the traffic that is

hidden1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with a virtual server instance, it controls the inbound and outbound traffic for the instance.

- **Virtual Private Network (VPN)**: A virtual private network provides the ability to extend the network perimeter with the use of encapsulation and encryption. Protocols such as IPsec, an extension to the IP, and secure sockets layer (SSL) are typically used with a web browser client. VPN is frequently used to provide secure communications over public networks to extend connections to remote locations such as branches or home office locations. This would enable secure connections while using the low cost of the Internet.
- **Virtual Private Cloud (VPC) (cloud environments)**: A VPC is a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of a cloud service provider.

While security would be sufficient on an Internet-based VPN, performance over the Internet cannot be guaranteed, and users may experience latency issues. Service providers may offer a private end-to-end IP network, which could have a VPN deployed to provide higher rates of delivery quality.

VPNs can also be used to provide access between business partners and organizations. Endpoints in a network might be governed by two entities with different requirements and security policies. VPNs enable secure communications regardless of levels of security within each standalone environment.

VPNs may be standalone hardware appliances, included in firewalls and routers, or software-based. Larger enterprises may have the equipment to manage many connections, such as large routers and switches. Router-based VPNs use the router's resources, whose primary purpose is to move traffic from one place to another. The router would need to be evaluated to ensure that traffic can still be effectively routed while increased processing is required to support VPN operations. Firewall-based VPNs would allow the VPN to terminate at the firewall so that the traffic packets could be inspected before routing the packets through the infrastructure. Software-based VPNs rely on a hardened operating system to provide secure communications. Because it is software-based, the performance of the device may be degraded due to encryption processes.

- **Web proxy**: A web proxy acts as an intermediary between a user accessing the web and a website. In the context of using the web, proxies are a way of accessing the web that provides another layer of anonymity. The fundamental way that proxies work is to mask the user's information from the sites they are attempting to access, which helps hide the user's identity.

Internal Network Protection

Protecting the internal network is equally important as protecting the network boundary, and many CISOs would argue it is even more important. CISOs must be familiar with the technologies available to see inside the network to detect threats and vulnerabilities.

- **Firewall (internal)**: An internal network firewall is not necessarily an innovative

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

technology but a specific application of the next-generation firewall platform. In most IT or hosted environments, the traffic patterns can broadly be described as follows:

- **North to South**: Traffic going from the LAN to the Internet, and vice versa.
- **East to west**: Traffic internal to the organization, routing server-to-server, server-to-client, or client-to-client but not leaving the organization.
- **Intrusion Detection System (IDS)**: An intrusion detection system gathers and analyzes information from computers or networks to identify security events and provide an alert. These devices are typically deployed at network perimeters or placed internally behind the firewall. IDSs operate continuously to protect the environment. IDSs may be signature-based, whereby the application or system vulnerabilities and the attack characteristics are codified to identify types of attacks. They may also be used to analyze behavior, searching for patterns beyond normal traffic baselines that cause it to send alerts. Signature-based IDSs do not detect zero-day attacks because signatures do not exist for the new attack method. IDS signature databases must be continually updated to provide adequate protection.

  IDSs may also be network-based or host-based. Host-based IDS systems typically consist of software installed on a host to check for system integrity changes such as file changes, registry settings, and CPU utilization to determine if an attack is occurring. Network-based IDS systems are composed of a management station and a sensor. Sensors are placed around the network to examine the traffic passing by and then send alerts to the management station when traffic matches a defined attack pattern.
- **Intrusion Prevention System (IPS)**: An intrusion prevention system examines network traffic flows to detect and actively stop exploits and attacks. IPSs identify potentially malicious traffic based on signatures or behaviors. Executables can also be seen (such as Trojan horses, backdoors, rootkits, and worms) and prevented from entering the network. Filtering and blocking traffic packets do this. IPSs are typically placed behind the firewall that is used to allow traffic that is supposed to pass and deny all that is not. Conversely, IPSs allow all traffic to pass except that which it detects and blocks due to a separate set of rules, such as the presence of executables.
- **Network encryption**: Network encryption encrypts or encodes data and messages transmitted or communicated over a computer network. It is a broad process that includes various tools, techniques, and standards to ensure that the messages are unreadable when in transit between two or more network nodes.
- **Transport layer security**: Many security protocols are performing encryption at various layers of the network model utilizing symmetric, asymmetric, and hashing algorithms to provide file integrity, message authentication, and confidentiality. Transport layer security (TLS) provides privacy and data integrity between two communicating applications on a network.

  TLS is the successor to SSL and is based on SSL version 3. TLS provides for mutual authentication of the server and client and is made up of two protocols to secure communications. These TLS Handshake Protocols create the connection using asymmetric and symmetric keys. The TLS Record Protocol maintains the integrity of the communications using a hash function.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network segmentation** is the act or practice of splitting a computer network into subnetworks, each being a network segment. The advantages of such splitting are primarily for boosting performance and improving security. This approach allows organizations to group applications and like data together for access by a specific group (for example, finance). It also limits the range of access provided to an insider, partner, or third party. Organizations have been forced to reevaluate their network access approach with increasing high-profile breaches. Some organizations implement network segmentation to comply with regulatory mandates such as HIPAA and PCI standards. Others know more considerable potential security risks are looming with a flat network. Regardless, business questions arise for all organizations, including how important it is to protect your brand, avoid lost sales, prevent stock losses, and avoid class action lawsuits.

3.5. Wireless (Wi-Fi) Security

Wireless networking uses radio waves to facilitate communication. Because of this, an attacker does not have to penetrate physical security defenses to gain access to the network. With sufficient power and a suitable antenna, an attacker can penetrate network defenses beyond the physical protection that protects access to a traditional wired network. This risk creates some unique concerns that the network security strategy in an organization must address.

3.5.1. Wireless Risks

Wireless network risks include:

- **Listening in**: Eavesdroppers can listen to network traffic and steal the authentication credentials of authorized users. Confidential information can be detected simply by analyzing wireless network traffic.
- **Stealing bandwidth**: Unauthorized individuals may connect to the wireless network to use the Internet without malicious intent. This may seem harmless, but they steal bandwidth from other users and could negatively affect network availability. If they are malicious, they could also use the connection against the company policy, send spam through the company mail server, or try to access other parts of the network.
- **Rogue access points**: Rogue access points are unauthorized wireless access points. They are added to the network but have not been authorized. Their primary concern is gaining access to the network or the Internet.

3.5.2. Wireless Controls

Business needs and the desire for mobility within an enterprise increase the likelihood that a CISO will have to define policies and procedures to manage wireless security. The requirements for securing a wireless network are like those for a wired network. Considerations for securing wireless networks include:

- **Administrative password**: Most access points come with a web-based interface that can be accessed to change the configuration settings. Default passwords must be changed, as they are widely known throughout hacker communities.
- **Media Access Control (MAC) address filtering**: Enabling MAC address filtering will block clients from joining that do not have a specified MAC address.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Service set identifier**: The service set identifier (SSID) is the network's name on the wireless router. Changing the SSID will slow the attacker because vendor-default SSIDs are readily known. The SSID broadcast can also be turned off, so the user would need to know the SSID to connect to it. These techniques may slow down the casual intruder looking for Internet access but will not stop an attacker from targeting access to the network. For instance, if the SSID is transmitted from a connected computer, it can be obtained by a hacker via eavesdropping.
- **Wi-Fi protected access 3 (WPA3)**: WPA3 is the most up-to-date wireless encryption protocol introduced in 2018 by the Wi-Fi Alliance. It incorporates various enhancements to its predecessors, WPA and WPA2, such as mandating the adoption of protected management frameworks to guard against eavesdropping and forging, disallowing obsolete security protocols, and standardizing the 128-bit encryption.

3.6. Voice over IP Security

The CISO must understand the unique security considerations for voice over Internet protocol (VoIP), which converts analog voice signals to digital information distributed over a packet-switched network. Attaching IP-based telephones to the network extends the attack surface that the CISO must manage. Attacks against this infrastructure may be used to commit fraud, disclose confidential voice communication, or facilitate other attacks to gain sensitive information from the network. Encryption, network segmentation, filtering, strong authentication, and other controls should be used in VoIP deployments to improve security.

Attackers can use virtual local area network (VLAN)-hopping attacks to exploit the weaknesses in the Layer 2 protocols to move between VLANs. By moving between VLANs, an attacker may use the VoIP system to access critical data such as credit card numbers and financial data.

Sniffing entails eavesdropping on unencrypted voice traffic. Hackers with access to VoIP can capture voice traffic with a sniffer tool, such as Wireshark, and convert the packets into a media file using a mechanism such as voice-over misconfigured Internet telephones. This enables hackers to listen in on sensitive voice communication.

hidoc.ir

4. ENDPOINT PROTECTION

Endpoint protection is the process of securing the various endpoints on a network or in-use by an organization, often defined as end user devices such as mobile devices, laptops, and desktop PCs. However, hardware such as servers in a data center are also considered endpoints. Precise definitions vary among thought leaders in security, but endpoint protection addresses the risks of devices connecting to an enterprise network.

Any device, such as a smartphone, tablet, or laptop, provides an entry point for threats. Endpoint protection aims to secure and protect every endpoint connecting to a network to block access attempts and other risky activity at these entry points. The enterprise network security perimeter has dissolved as more enterprises adopt practices such as BYOD (bring your own device) and remote/mobile employees.

The need for effective endpoint protection measures has increased, particularly considering the rise in mobile threats. With employees relying on mobile devices, home computers, and laptops to connect to company networks and conduct business, a centralized security solution is no longer adequate for

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

today's ever-shifting and undefinable security perimeter. Endpoint protection supplements centralized security measures with additional protection at the point of entry for many attacks and the point of egress for sensitive data.

Endpoint protection products may contain features and functionality such as:

- Data loss prevention.
- Insider threat protection.
- Hard drive, endpoint, and email encryption.
- Application whitelisting or control.
- Network access control.
- Data classification.
- Endpoint detection and response.
- Enhanced memory analysis and protection.
- Privileged user control.
- Support for extensible threat hunting protocols (e.g. STIX/TAXII/YARA etc.)

Endpoint protection is, however, not solely conducted from devices. Typical endpoint protection solutions provide a two-pronged approach, with software installed on a central server or management console and software installed on individual devices.

hide01.ir

4.1. Endpoint Threats

Malware: Malware does damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software. The code is described as computer viruses, worms, trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user—and so does not include software that causes unintentional harm due to some deficiency, typically described as a software bug.

- **Viruses**: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected."
- **Ransomware**: Ransomware is a type of malware that restricts access to the infected computer system and demands that the user pay a ransom to the malware operators to remove the restriction.

Phishing attacks: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a homophone of fishing due to the similarity of using bait to catch a victim. Phishing attacks traditionally use emails as the distribution channel. These have evolved to include channels such as QR codes (squishing), voice messages (vishing), and text messages (smishing). Spear phishing and whaling are more sophisticated and targeted email phishing attacks, often aimed at high-value targets such as company executives.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4.2. Endpoint Vulnerabilities

Bring Your Own Device (BYOD): Because of the broad range of devices that employees might use to perform their job duties, there is the potential for an increase in the amount vulnerable code being brought into the company.

Inadequate security patching: Enterprises should apply best practices for patching, which require test environments for any systems included in patch management endeavors. The enterprise should use policies to automate pushing tested patches out to devices, which typically occurs within a week of satisfactory test completion.

Incomplete application blocking: Adjust application control to your device fleets and roll out blocklisting/allowlisting tools gradually to address each endpoint's unique needs and appropriately deny applications by default.

Shadow IT: Potential for growing vulnerabilities within the IT landscape with the increasing use of IT-related systems and services without the knowledge or authorization from the organization's IT department.

4.3. End User Security Awareness

Endpoint protection begins with the user or the human firewall. The human factor is the underlying reason many cyberattacks are successful. Distraction, ignorance, and curiosity are just some factors that can lead to high-risk behavior regarding security. Most end users are cybersecurity agnostic. That is to say, they won't actively seek to break cybersecurity policies, but should a policy or procedure prevent them from completing their work, they are more likely to break such a policy/procedure. CISOs, therefore, need to structure an effective, innovative, and relevant security awareness program to leverage this first line of defense. Security technological defenses can only protect endpoints to a certain point; users require training to not unwittingly allow bad actors into the enterprise. As a CISO, you must educate users on privacy and security controls. This is especially important considering the remote work/work-from-home movement, where users can access sensitive information from anywhere.

To assist in the creation of an effective security awareness program, the following guidelines may be helpful:

- **IS policies**: Policies should be understandable and relevant to the user's position. Complicated and lengthy policies can do more harm than good. Users should know within minutes of reading a policy what they are allowed and not allowed to do with organizational information and assets.
- **Security awareness portal**: A security awareness portal is a valuable resource to communicate policies, best practices, and safety tips throughout an organization.
- **Security awareness communication plan**: Keep-it-simple is ideal for communicating security awareness messages to end users. This approach recognizes that users are hired for their specific expertise, not cybersecurity expertise, yet still need to understand the critical concepts of avoidance, privacy, and information protection. There must be a balance in the timeliness of communications to keep the end user community interested and alert.
- **Integrate security responsibilities into user responsibilities**: Users' roles and responsibilities related to security should be formalized in their job descriptions.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **User security incentives**: Security should not be punitive but rather incentivized to shape the behavior required of users to serve as the first line of security defense.
- **Security awareness training**: Training should be short, interactive, and timely. Senior leadership should be involved, and advanced training techniques such as phishing testing and surveys should be implemented.

4.4. Endpoint Device Hardening

In computing, hardening is usually the process of securing a system by reducing its surface vulnerability, which is more significant when a system performs more functions; in principle, a single-function system is more secure than a multipurpose one.

Hardening settings can be applied as determined by recognized industry standard frameworks ad guides such as the CIS Benchmarks and NIST National Vulnerability Database for operating systems and standard applications.

- Enable inherent OS encryption.
- Restrict applications.
- Apply applicable OS and application patches.
- Uninstall unnecessary software and utilities.
- Disable unnecessary ports and services.
- Perform vulnerability scanning.

hide01.ir

4.5. Endpoint Device Logging

Many applications record errors and events in proprietary error logs, each with its own format and user interface (UI). Data from different applications cannot be merged into one complete report, requiring system administrators or support representatives to check various sources to diagnose problems.

Event logging provides a standard, centralized way for applications (and the operating system) to record essential software and hardware events. The event logging service records events from various sources and stores them in a single collection called an event log. The event viewer lets you view logs; the programming interface also enables you to examine logs.

4.6. Mobile Device Security

Mobile security protects smartphones, tablets, laptops, and other portable computing devices and the networks they connect to from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security although the two focus areas overlap, they are different.

4.6.1. Mobile Device Risks

The Open Web Application Security Project (OWASP) top 10 mobile device risks, as finalized in 2016, are listed below [94]. The list is being updated for 2023, and it is good practice for CISOs to ensure the most up-to-date lists are referenced.

- **M1: Improper platform usage**: This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

part of the mobile operating system. There are several ways that mobile apps can experience this risk.

- **M2: Insecure data storage** covers insecure data storage and unintended data leakage.
- **M3: Insecure communication**: This covers poor handshaking, incorrect SSL versions, weak negotiation, clear-text communication of sensitive assets, etc.
- **M4: Insecure authentication**: This category deals with authenticating end users and poor session management. These include:
    - If the mobile app is able to anonymously execute a backend API service request without providing an access token, this application suffers from insecure authentication.
    - If the mobile app stores any passwords or shared secrets locally on the device, it most likely suffers from insecure authentication.
    - If the mobile app uses a weak password policy to simplify entering a password, it suffers from insecure authentication; or
    - If the mobile app uses a feature like TouchID, it suffers from insecure authentication.
- **M5: Insufficient cryptography**: This category is for issues where cryptography was attempted but was implemented incorrectly.
- **M6: Insecure authorization**: This category captures any failures in authorization (for example, authorization decisions on the client side and forced browsing). It is distinct from authentication issues (for example, device enrolment and user identification). Suppose the app does not authenticate users in a situation where it should (for example, granting anonymous access to some resource or service when authenticated and authorized access is required). In that case, that is an authentication failure, not an authorization failure.
- **M7: Client code quality**: This is the catch-all for code-level implementation problems in the mobile client. This is distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level errors where the solution is to rewrite some code running on the mobile device.
- **M8: Code tampering**: This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. The code and data resources reside there once the application is delivered to the mobile device. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system application programming interfaces (APIs) the application uses, or modify the application's data and resources. This can provide the attacker with a direct method of subverting the intended use of the software for personal or monetary gain.
- **M9: Reverse engineering**: This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, and other binary inspection tools give the attacker insight into the application's inner workings. This may exploit other nascent vulnerabilities in the

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

application and reveal information about back-end servers, cryptographic constants and ciphers, and intellectual property.

- **M10: Extraneous functionality**: Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally have a password as a comment in a hybrid app. Another example includes disabling multi-factor authentication during testing.

4.6.2. Mobile Device Security Controls

NIST guides Mobile Device Management (MDM) in its Special Publication 800-124 Revision 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise [95]. NIST also provides a practical reference architecture for deploying MDMs in an enterprise via NIST SP 1800-4 [96], which also contains an example policy set for MDM/Enterprise Mobility Management (EMM) policies. Various settings can be implemented, some of which may be overly restrictive depending on the use case.

Examples of policies that can be instituted using EMMs include:

- Strict regulation of applications using allowlists/blocklists.
- Automated response to application noncompliance, such as notifications, enterprise data wipe, profile removal (for example, email), profile installation (for instance, restrictions), and managed application removal.
- Require end users to upgrade to a compliant OS and send notifications to devices to prompt upgrades and patches.
- Restrict device settings through over-the-air profiles.
- Restrict the use of device hardware features such as a camera, secure digital (SD) card, USB, Bluetooth, tethering, and more.
- Disable access to public application stores.
- Disable carrier preinstalled apps, such as Facebook.
- Control Wi-Fi, hotspot, and other network security settings.
- Disable content sharing, for example, using the copy-paste function, emailing, printing, and opening content with specific applications.
- Configure email security settings, including turning off the copy-paste function and SD card access.

4.7. Internet of Things Security (IoT)

The Internet of Things (IoT) is the network of physical objects - devices, vehicles, buildings, and other items - embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The spending on IoT across key industries reached over $268 billion in 2022. IoT devices are forecast to grow at a compound annual growth rate of 15% from 2021 through 2025 [97].

IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones, and tablets, to any range of traditionally *dumb* or non-Internet-enabled physical and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

everyday devices. Embedded with technology, these devices can communicate and interact over the internet and be remotely monitored and controlled.

The main problem with IoT devices is that their manufacturers quite often need to be faster to implement security functionality. Many devices, like security monitoring cameras, are produced as inexpensively as possible and equipped with essential software, which often cannot be updated and has no built-in security controls or functionality. Some of the IoT security challenges include:

- Weak authentication and authorization.
- Lack of encryption.
- Vulnerabilities in firmware and software.
- Insecure communication sessions.
- Difficulty in patching and updating devices.

4.7.1. Protecting IoT Devices

Several significant IoT attacks have heralded a new threat vector for CISOs. These Internet-connected devices create access points with which hackers can infiltrate a company's network. Due to the wide range of devices and technologies, it is challenging to implement a cohesive security strategy. Such attacks present a dual-edge problem for organizations as users can use their IoT devices to attack other companies. In October 2016, for example, a massive DDoS attack using IoT devices attacked a DNS service provider. It brought down substantial portions of the internet, including sites such as Amazon, Netflix, and Twitter. IoT devices with outdated firmware or weak default passwords were infected with the Mirai malware to create the IoT botnet network used for the attack.

The following are essential steps that CISOs must take to protect their IoT devices:

- **Inventory IoT devices**: Organizations must know where their devices are deployed on the network. Extending an existing information security plan to protect IoT devices will only be possible by knowing their location.
- **Security test IoT devices**: Many devices have been rapidly manufactured to gain market position. This results in little time and resources to thoroughly security test these devices. This results in the responsibility of security testing falling on the CISO's doorstep.
- **Revise IS policies**: Each policy should be reviewed, considering IoT devices to validate their appropriateness. IS policies should clearly state which IoT devices are allowed and what type of data exchanges are permissible on the network.
- **Define an inclusive IoT architecture**: IoT devices can be deployed anywhere, and traditional security designs may no longer apply. However, the same concepts of security do apply. For example, IoT devices require access control, encryption, hardening, monitoring, and most other IS disciplines.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. APPLICATION SECURITY

A crucial role of the CISO is the evaluation of vulnerabilities in an organization. To that end, the CISO must remain engaged with organizational teams managing systems and applications to ensure that vulnerabilities do not create unnecessary risks for the organization. System and application security are concerned with managing the data-processing assets of an organization by enforcing secure development, implementing secure configurations, and minimizing vulnerabilities.

5.1. Secure SDLC Model

A secure Systems Development Life Cycle (SDLC) model is a process that has security touchpoints in every stage, as well as security milestones. Secure SDLCs go beyond the current SDLC structure to ensure the deployed applications are secure upon release without delaying the original SDLC.

The following is a representation of the secure SDLC model:

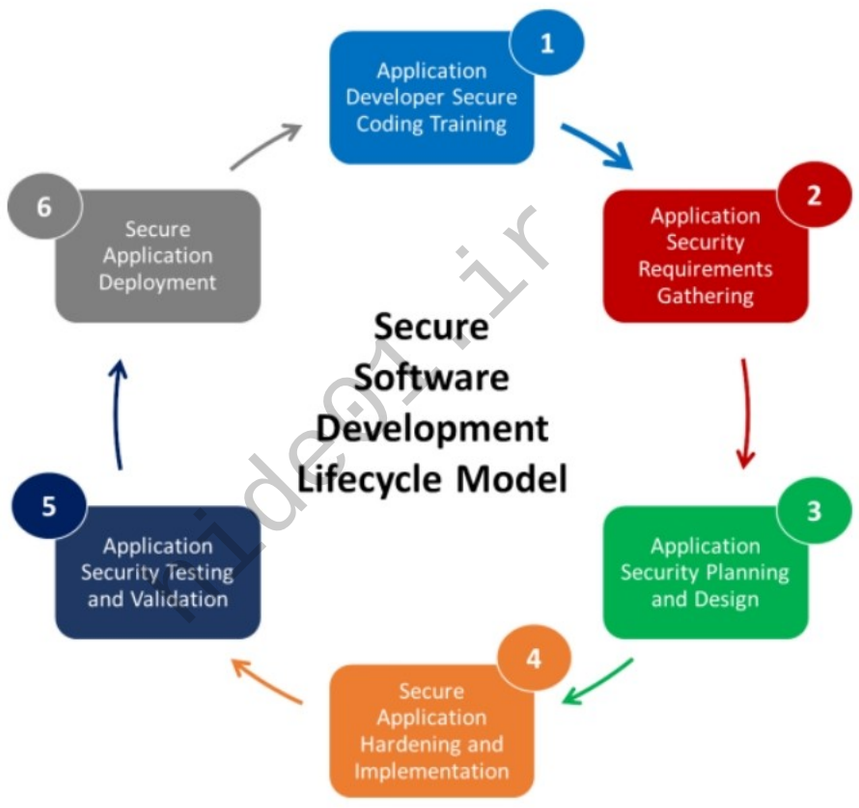


Figure 51: Secure SDLC Model

5.2. Separation of Development, Test, and Production Environments

Software engineers should have more access to the test and development environments than production environments. This is to preclude the possibility of system compromise, ensure the reliability of production assets, and maintain suitable environments to evaluate features. Joining test and production environments can expose production data to test code that may not be secure. This can result in access to a production system and its data, creating unwanted exposure. Performance degradation could also result; untested queries could consume the capacity of a server, causing a production application to get fewer throughputs than expected.

Live data is sometimes used for testing. This practice should be discouraged because developers usually do not need access to critical or sensitive data to develop and evaluate a program. A better technique is to mask or scramble key identifying information for testing. Sometimes, this isn't easy with large, complex systems where fundamental values or data relationships must be retained to provide quality assurance.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5.3. Application Security Testing Approaches

Under ideal conditions, security is provided throughout all phases of the SDLC. Dynamic and static application testing offers an opportunity to evaluate the effectiveness of the designed system's security controls.

- **Dynamic application security testing (DAST)**: This testing technique simulates a malicious attacker's activities while a system is running or in a dynamic state. This process involves sending various inputs to a web application and analyzing the response to uncover potential vulnerabilities.
- **Static application security testing (SAST)**: This is an examination of source code, bytecode, or binary code performed either manually or by automated code review tools to uncover design flaws and coding errors. Automated software testing tools can quickly identify potential issues and, in some cases, provide information to fix code flaws. SAST performs well when finding an error in a line of code, such as weak random number generation, but is usually inefficient in finding data flow flaws.
- **Fuzz testing tools**: A software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of an application. The application is then monitored for exceptions such as crashes or failing built-in code assertions or for finding potential memory leaks.
- **Interactive application security testing (IAST)**: This solution analyzes the behavior and interactions of applications in real-time and during runtime using agent-based monitoring. This technique allows IAST to combine the strengths of both SAST and DAST methods and provide access to code, HTTP traffic, library information, back-end connections, and configuration information. Some IAST products require the application to be attacked, while others can be used during routine quality assurance testing.
- **Penetration application security testing**: The primary objective of a web application penetration test is to identify exploitable vulnerabilities in applications before hackers can discover and exploit them. Web application penetration testing will reveal real-world opportunities for hackers to be able to compromise applications in such a way that allows for unauthorized access to sensitive data or even take over systems for malicious/non-business purposes.
- **Bug bounty program**: A bug bounty program is an agreement the organization offers to encourage external security researchers to responsibly search and report on security vulnerabilities and bugs in exchange for recognition and compensation.

The CISO can use these approaches to increase the organization's understanding of the importance of reviewing its code. It also assures that the code or system will not be exploited once deployed. The tools can also validate that secure coding practices have been followed. Automated tools can reduce the workforce necessary to review source code.

5.4. DevSecOps

One of the newest ways to operationalize cybersecurity is to integrate security within your organization's development operations (DevOps). DevOps is a term used to describe the integration of application development with IT operations or the breaking down of the silos that exist between application developers and IT operations personnel. A lack of communication

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

between application developers and IT operations has been a root cause of many security vulnerabilities. Developing applications in a vacuum and then tossing them over to IT operations to run is not effective, sustainable, or, most importantly, secure.

CISOs may find the best way to view DevOps is to think of it as a way for application development teams and IT operations personnel to work together during the entire application development lifecycle from design through development to production. DevOps results in a practice of continuous integration and continuous deployment versus the former "big bang" approach to launching applications, leading to faster and more reliable application development.

CISOs can embrace the DevOps movement and leverage it to improve the cybersecurity of one of the most significant exposure areas of an organizations attack surface: applications. Approached correctly, DevOps can significantly improve your organization's cybersecurity practices. One of the main benefits of DevOps is acquiring and acting on application functionality feedback earlier rather than later in the development cycle. This translates to improved cybersecurity, where you can detect application security flaws earlier in the development and deployment phases, enabling your organization to respond faster to vulnerabilities. But you must understand your organization's DevOps and learn about some unique technologies enabling DevOps, such as containers and microservices.

DevOps is a disruptive technology that has changed the application development landscape, operations, and security. Connecting cybersecurity with DevOps integrates security testing, validation, and monitoring throughout the application development lifecycle to deployment. By providing application developers with automated cybersecurity tools and placing them in charge of their destiny, cybersecurity is no longer blamed as the gatekeeper.

In 2012, Gartner introduced the concept of DevSecOps (MacDonald & Head, 2016), creating the linkage between DevOps and security. According to Gartner, by 2023, more than 70% of enterprise DevSecOps initiatives will have incorporated automated security vulnerability and configuration scanning for open-source components and commercial packages, which is a significant increase from fewer than 30% in 2019. You will most likely want to ensure you are in the 70% camp and engage cybersecurity with your DevOps efforts given its cybersecurity benefits.

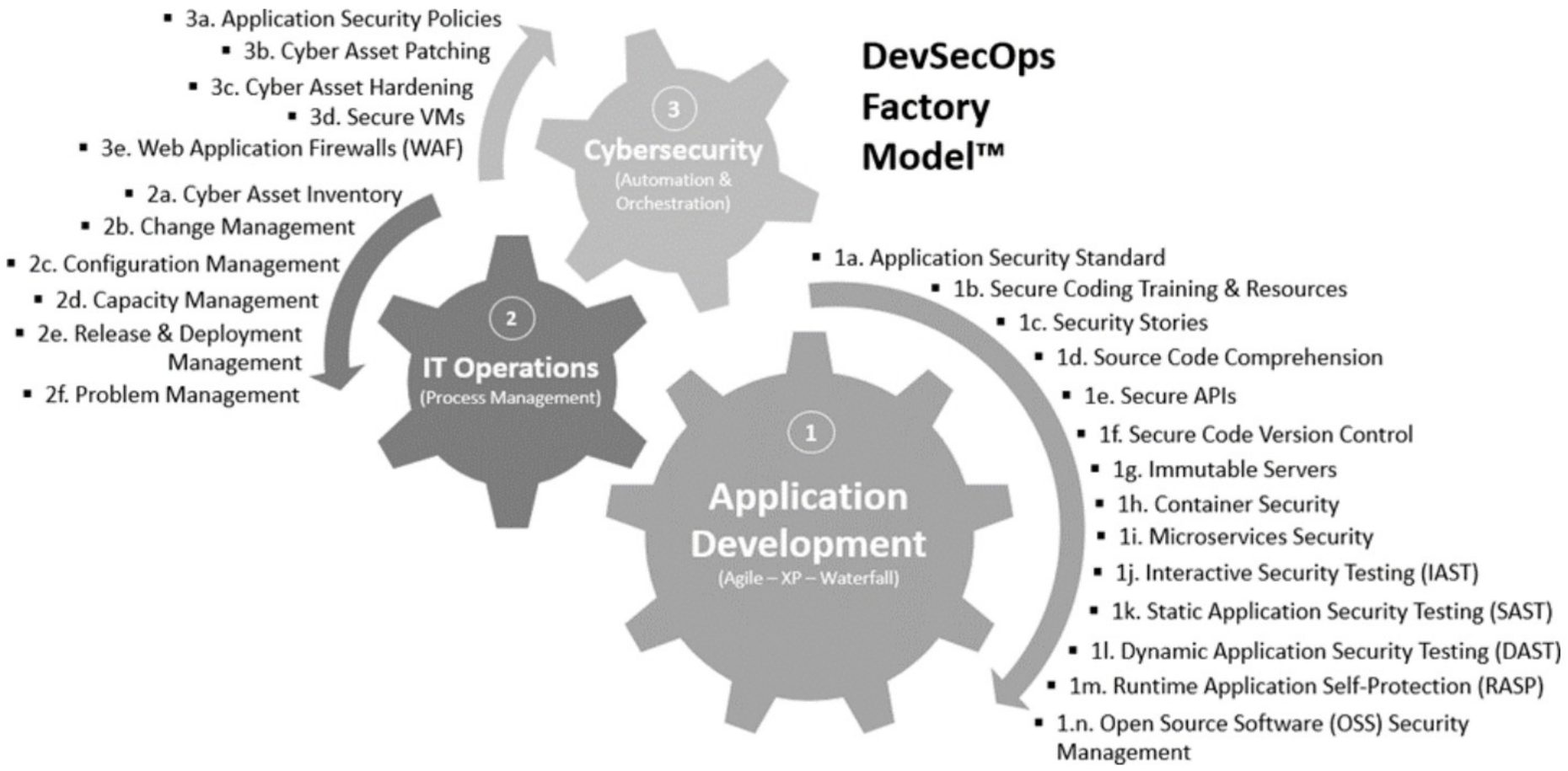


Figure 52: DevSecOps Factory Model™ (By Tari Schreider, licensed under a Creative Commons Attribution-Non- Commercial-NoDerivitives 4.0 International License).

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5.5. Waterfall Methodology and Security

The waterfall model is a sequential design process used in software development processes in which progress flows steadily downward (like a waterfall) through the phases of conception, initiation, analysis, design, construction, testing, production/implementation, and maintenance. The waterfall model includes five phases within which work artifacts are produced, reviewed, refined, and approved. The model reflects a waterfall because no opportunities exist to return to a previous phase once the phase is complete. Like a waterfall, you must keep moving forward until you reach the destination.

- **Requirements**: All requirements, outcomes, and features related to the intended system are documented in this phase. The requirements phase provides a roadmap for the rest of the SDLC effort.
- **Design**: Developers model requirements as features, modules, and other components supporting the solution defined in the requirements phase. The design phase helps define the system, environment, and enterprise architectures required to support the final solution.
- **Implementation**: Activities completed in the requirements and design phase are combined to create the system.
- **Verification**: The system created in the implementation phase is evaluated to verify that all features, functionality, and capabilities defined in the requirements phase are present in the system and working as intended. The system moves into production once verification is complete.
- **Maintenance**: The maintenance phase relates to change management and the processes that govern the changes made to hardware, software, and documentation that support the system's operational effectiveness.

hideo1.ir

The following is a representation of a secure waterfall methodology:

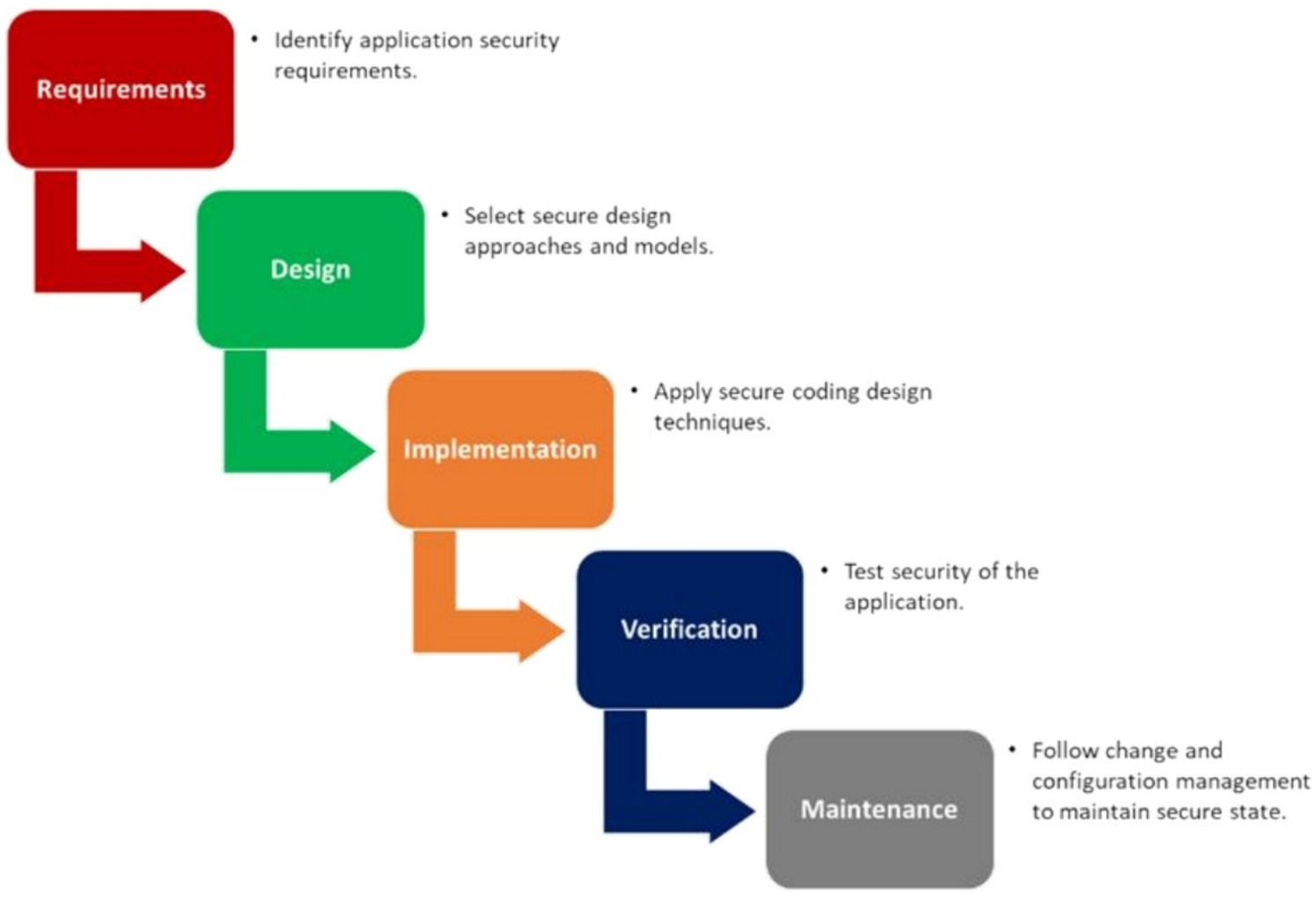


Figure 53: Secure Waterfall Diagram

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5.6. Agile Methodology and Security

Introduced in 2001 by a group of software developers that created the Agile Manifesto, this process calls for teams to develop working software at the end of short periods, which are typically four weeks. To achieve this result, there must be continuous collaboration with the customer for potential requested changes. Agile has replaced the Waterfall methodology in modern software development due to its shorter feedback loop and tremendous success in achieving customer objectives.

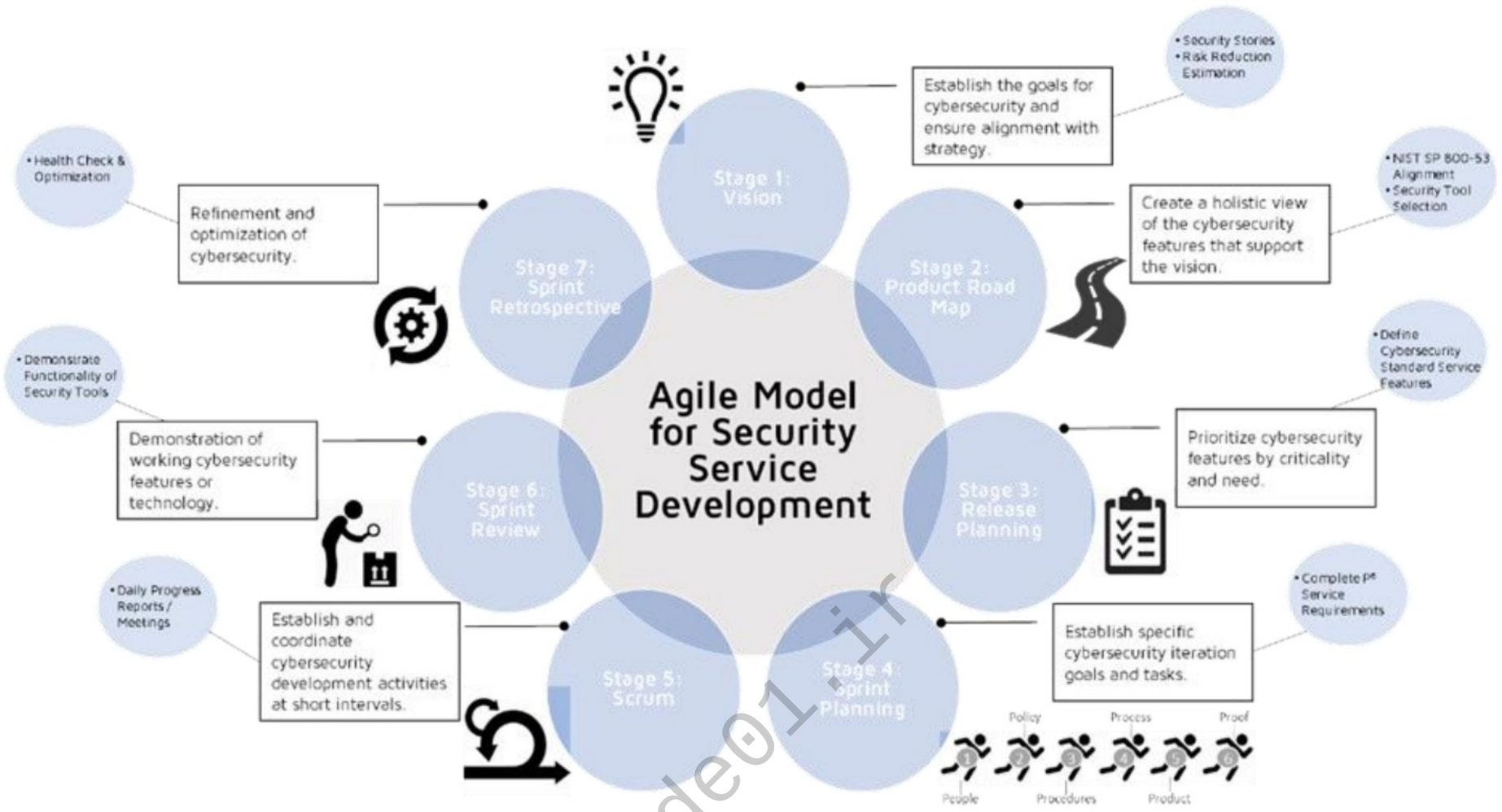


Figure 54: Agile Security Model

5.7. Other Application Development Approaches

- **Joint application development**: Joint application development or JAD is a team-oriented approach that involves the customer and technology departments working together to capture the user's view of the business requirements before developing the system. This process is used to determine the requirements for complex systems.
- **Prototyping method**: Sometimes referred to as a "proof of concept (PoC)," this method is typically used to determine system requirements before committing more significant amounts of money to an effort. The system's functionality and feasibility can be discovered before developing the system to meet the needs on a larger scale.

5.8. Application Hardening

Applications are challenging to secure due to their complexity and ability to accept input from many dissimilar sources using potentially various levels of access and authority. Applications not being used should be removed, as exploits may be written for old code, the code may no longer be supported, and patches are no longer being developed for it. Externally facing web applications are particularly vulnerable as they are readily accessible.

Application hardening involves various procedures to prevent attacks by fixing vulnerabilities and removing or disabling nonessential functionality or components. The phrase application hardening is about various methods for protecting a computer system. Security is provided in

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

layers and is often called "defense-in-depth." Layers of protection mean protecting the host level, the application level, operating systems, the user level, the physical level, and the various sublevels between each. Every level requires unique security defense methods.

Hardening a system includes a few stages to shape layers of assurance. It ensures secure processing and protection layers to secure systems inside and out. Hardening provides an in-depth and comprehensive defense.

5.9. Application Security Technologies

Secure coding can only go so far in protecting an application; additional technologies may need to be applied to protect applications from further exploitation.

- **Application Programming Interface (API) manager**: Security is an essential element of any application, especially to APIs, where hundreds or thousands of applications make calls daily. New threats and vulnerabilities are created every day, and companies find themselves racing against the clock to patch them. It is crucial to protect your APIs from attacks. An API Gateway or API manager can be an intermediary between clients and APIs, handling authentication, authorization, traffic management, rate limiting, and logging and monitoring. While an API manager does not remove all threats, it can help protect against some of the most common ones.
- **Runtime Application Security Protection**: As with IAST, runtime application security protection (RASP) works inside the application, but it is less a testing tool and more a security tool. It is plugged into an application or its runtime environment and can control application execution. RASP allows an app to run continuous security checks on itself and respond to live attacks by terminating an attacker's session and alerting defenders to the attack.
- **Software Composition Analysis**: A set of tools that provides users visibility into their open-source inventory. Despite its misleading name suggesting access to all aspects of the source code (proprietary, third-party commercial, and open source), software composition analysis (SCA) only acts as an open-source management tool. SCA tools generate an inventory report of all open-source components in your products, including all direct and transitive dependencies. Inventory of open-source usage is critical as it is the basis for effectively managing it.
- **Web Application Firewall**: A software solution that filters, monitors, and blocks HTTP/HTTPS traffic to and from a web application. A web application firewall (WAF) is differentiated from a regular firewall in that a WAF can filter the content of specific web applications. In contrast, traditional firewalls serve as a safety gate between servers. Inspecting HTTP/HTTPS traffic can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting, file inclusion, and security misconfigurations.

5.10. Version Control and Patch Management

- **Patch management**: Applications are used in business for many reasons. Whether you use Skype or Zoom to contact work-from-home employees or use Adobe for portable data files, you are using third-party applications and need to ensure the safety and integrity of your computer system. Many of these apps are not considered entirely safe, so when you download them, you could be opening your doors to phishing, malware, or viruses.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To help with that, patches are offered, but your IT group must know when and where to find them, install them, and evaluate them.

- **Version control**: A component of software configuration management, version control, also known as revision control or source control, is the management of changes to documents, computer programs, large websites, and other collections of information. Changes are usually identified by a number or letter code, termed the "revision number," "revision level," or simply "revision."

5.11. Database Security

Database security concerns are broad and involve a range of information security controls to protect databases against confidentiality, integrity, and availability compromises. It involves several types or categories of controls, such as technical, procedural/administrative, and physical. Database security is a specialist topic within computer security, information security, and risk management.

- **Isolate sensitive databases**: Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing in those databases.
- **Harden databases to the fullest extent possible**: Clearly, it is vital to ensure that the database you are using is still supported by the vendor or open-source project responsible for it and that you are running the most up-to-date version of the database software with all database security patches installed to remove known vulnerabilities.
- **Remove vulnerabilities**: Continually assess, identify, and remediate vulnerabilities that expose the database.
- **Deploy database firewalls**: Database firewalls are a type of WAF that monitors databases to identify and protect against database-specific attacks that primarily seek to access sensitive information stored in the databases. Database firewalls also enable monitoring and auditing of all database access through their logs.
- **Encrypt the data**: It is standard procedure in many organizations to encrypt stored data. However, it is essential to ensure that backup data is encrypted and stored separately from the decryption keys. Not, for example, stored in encrypted form but alongside the keys in plaintext. Apart from encrypting data-at-rest, it is also essential to ensure confidential data is encrypted in motion over your network to protect against database security threats.
- **Enforce least privilege access**: Identify user entitlements and enforce user access controls and privileges to limit access to only the minimum data required for employees to do their jobs.
- **Monitor for deviations**: Implement appropriate policies and monitor any vulnerabilities that cannot be remediated for all activities that deviate from authorized activity.
- **Audit and monitor database activity**: This would include monitoring sign-ins (and attempted sign-ins) to the operating system and database and reviewing logs regularly to detect anomalous activity. Effective monitoring should allow you to spot when an account has been compromised, an employee is conducting suspicious activities, or your database is under attack. It should also help you determine if users are sharing accounts and alert you if accounts are created without your permission (for example, by a hacker).

  Database activity monitoring software can help with this by providing monitoring

n1oe01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

independent of native database logging and audit functions; it can also help monitor administrator activity.

- **Respond to suspicious behavior**: Alert and respond to any abnormal or suspicious behavior in real-time to minimize attack risk.

5.12. Database Hardening

Most of the critical information in an organization is stored in a database. Effective security hardening of databases is vital to reduce vulnerabilities and improve risk status—database operating systems function analogously to server and endpoint operating systems. Therefore, the tools, techniques, and processes used to achieve system hardening, in general, often apply to hardening and protecting database systems.

Database hardening is not limited to the server on which the database resides. The database security strategy should ensure applications accessing the database are also evaluated for the effectiveness of their security controls.

5.13. Secure Coding Practices

Securing coding is the practice of developing computer software to guard against the accidental introduction of security vulnerabilities. Defects, bugs, and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities.

The following is a compendium of secure coding practices your organization should adopt:

- **Adopt a secure coding standard**: Using OWASP or a similar source applicable to your programming languages. Train developers to the standard and create enforcement policies to further the adoption of the standard.
- **Define application security policies**: Publish security policies that support and enforce secure coding design and your organization's application development framework or architecture.
- **Define application security requirements**: Each application or language should have documented security requirements created early in the development life cycle. Verify that the requirements are upheld as the applications go through the SDLC.
- **Adopt minimalist coding philosophy**: Keep application design as simple and small as possible. The more lines of code and the more complex the code, the more threat vectors and errors that are created.
- **Apply the principle of least privilege**: Applications should operate on a least privilege basis, with every process executing with the least privileges necessary to complete the job.
- **Deny access by default**: Design application access to deny all access. Application owners should grant access permission rather than exclude access.
- **Validate input**: Applications should be designed to validate input to remove most software vulnerabilities.
- **Heed compiler warnings**: Compile code using the highest warning level available for your compiler and remove warnings by modifying the code.
- **Sanitize data sent to other systems**: Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf components.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. ENCRYPTION TECHNOLOGIES

The CISO should be familiar with encryption's various processes, technologies, and tools, an essential security control supporting confidentiality.

6.1. Encryption and Decryption

Encryption encodes a message or information so only authorized parties can access it. Encryption does not prevent interference but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, or plaintext, is encrypted using an encryption algorithm - a cipher - generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Decrypting the message without possessing the key is possible, but considerable computational resources and skills are required in order to do so for a well-designed encryption scheme. An authorized recipient can decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

6.2. Cryptosystems

A cryptosystem is a suite of cryptographic algorithms needed to implement a security service, most commonly for achieving confidentiality (encryption). Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption.

6.2.1. Blockchain

Blockchain is an expanding list of records called blocks linked cryptographically as a chain. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. This makes it one of the most secure methods to perform transactions. The concept is that an open-distributed ledger records transactions between parties while maintaining their anonymity. This approach is safe because the transaction record cannot be altered in any one block without altering all previous blocks. The credit for the development of blockchain goes to Satoshi Nakamoto in 2008. Blockchain was designed to serve as the public transaction ledger of the cryptocurrency Bitcoin.

Blockchain is now used to secure sensitive records utilizing keyless signature infrastructure to replace the more traditional public key infrastructure (PKI), which uses asymmetric encryption and a cache of public keys maintained by a centralized certificate authority (CA). In 2016, this technology was used to secure all of Estonia's 1 million health records [98].

6.2.2. Digital Signatures and Certificates

Digital signatures provide a mechanism to verify that a message came from the sender, providing nonrepudiation. This means someone sending a file or providing a digital signature cannot later claim they did not. Here is the basic process:

- A hash, or message digest, is created from the message the person wants to send.
- The message digest is encrypted with the sender's private key.
- The recipient decrypts the message digest using the sender's public key.
- The message digest is recomputed for the file.
- The on-system message digest is compared to the message digest that was sent earlier.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the recipient can open the message with the public key, then the message could only have been sent by the sender, who encrypted the message with the private key. If the recomputed message digest matches the one sent, then the file integrity is intact.

- Asymmetric algorithms are more computing-intensive than symmetric algorithms; for this reason, asymmetric and symmetric algorithms are used in conjunction with each other. For example, if a message requires nonrepudiation, the digital signature can be generated by creating the message digest much faster than encrypting the entire message using the private key. The contents of the message can be encrypted using symmetric algorithms. Then, the symmetric key can be provided using public/private key encryption. In this manner, the entire message is encrypted, and the symmetric or secret key is delivered securely.

6.2.3. Public Key Infrastructure (PKI)

PKI provides the mechanisms that ensure public keys belong to who they say they do. The framework permits individuals and applications to interact with each other to verify their identity as a trusted source. Directories of public keys may be managed, or a trusted CA may issue digital certificates. The certificate would identify the individual or company in the transaction with other details that the CA has verified. The digital certificate is digitally signed by the CA using a hash of the certificate with the CA's private key. The certificate then provides a mechanism by which the individual's public key can be associated with the individual's identity and, therefore, be trusted.

6.2.4. Key Management

Modern cryptography is based on mathematical formulas; the algorithms could be broken given adequate time and resources. However, this is not practical for many algorithms with current technologies. The weakest link in the existing encryption chain is the security of the keys. Keys may be stored centrally and use a facility such as a key distribution center, where cryptography is used to distribute session keys in an encrypted manner.

Utilizing a hardware security module (HSM) is another option. An HSM is a physical computing device that safeguards and manages secrets (most importantly digital keys), performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. A hardware security module contains one or more secure crypto processor chips.

If a key is lost, there may only be the means to recover if it was provided to someone in the IT department as part of a policy. Some encryption products offer alternate means of retrieving data in case of a lost key. Keys should also be protected while in storage using strong access controls and securely archived for future retrieval.

External providers of IT services may want to avoid taking on the legal liability of losing encryption keys. They sometimes establish clauses in their contracts designating a department, usually the IT service delivery or the information security program, as responsible for managing the keys.

nilde01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.3. Hashing

Hashing is an integrity control. Hash functions perform a one-way transformation of a string of characters into a fixed-length value or key that represents the original string. The fixed-length files are small, typically 128 bits in size. These are considered one-way functions because the hash, sometimes called a message digest, cannot be used to regenerate the original message. It provides a small representation of the source files. These common types are message-digest algorithm version 5 (MD5) and secure hash algorithm-1,2 and 3 (SHA-1, -2, -3).

6.4. Encryption Algorithms

Encryption algorithms change plaintext information into cipher text. The decryption process is reversible by using a key to transform the cipher text back into plaintext. Symmetric encryption and asymmetric encryption are the two primary encryption approaches. Both require protecting critical information to maintain confidentiality within the encryption process.

- **Symmetric encryption**: Symmetric key encryption uses an algorithm that uses a single, shared key to encrypt and decrypt the message. Symmetric key encryption is also called private key, shared key, secret key, single key, or same key encryption. One party encrypts the message using a key, and the receiving party decrypts the message using the same key. The limitation of this approach is that the key must be securely shared with the party that will be decoding the message. This usually means supplying an unencrypted message, typically through a different means than the message was delivered—such as fax, voicemail, overnight delivery, or in person.

  The 56-bit key data encryption standard (DES) and the 128, 192, or 256-bit advanced encryption standard (AES) are examples of symmetric key algorithms. The DES is not considered a substantial encryption standard today, as it only took 56 hours to determine the key through a brute force attack in 1998. The AES subsequently replaced the DES; the 3DES (triple DES) is more robust and used in many products today but it is less secure than AES. AES-256 is the recommended algorithm currently.

  Symmetric encryption key management in an enterprise system is an issue due to the number of keys necessary to exchange information. If an organization had 50 users, it would need to maintain 1225 keys to exchange data securely with each other. The formula for the number of keys required for n users is $n(n - 1)/2$. The other difficulty with symmetric encryption is that when keys are shared between several people for the same file, there is no ability to determine who accessed or changed the file.

- **Asymmetric encryption**: Asymmetric encryption was successfully demonstrated with the Public Key Diffie–Hellman Algorithm introduced in 1976 and the RSA Algorithm (Rivest, Shamir, and Adelman) in 1977. Asymmetric encryption is also known as public/private key encryption. It uses keys in pairs to encrypt and decrypt information. One of the keys is kept secret and is called the private key, while the other is made public and known as the public key.

  An individual can send a message to another individual by encrypting the message with the recipient's public key. Because the keys are in pairs mathematically linked by factors of large prime numbers, the only key to decrypt the message is the recipient's private key for that public/private key pair. This provides integrity and confidentiality, as the message cannot be decrypted with only the private key. This differs from symmetric key encryption,

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

where the same key is used to encrypt and decrypt. The advantage of this approach is that a secret key does not have to be shared, thus solving the problem of sharing the symmetric keys.

- **Elliptical curve cryptography**: A public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. Elliptical curve cryptography generates keys through the properties of the elliptic curve equation instead of the traditional generation method as the product of large prime numbers.

  Elliptic curves are applicable for key agreements, digital signatures, pseudo-random generators, and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme.

6.5. Encryption Strategy Development

CISOs must develop an encryption strategy to determine the most appropriate algorithm to protect sensitive information. Legal requirements also drive strategies for encrypting information. Key management and whether multiple keys would be required to protect data from access by court order must be considered.

6.5.1. Determining Critical Data Location and Type

Unprotected data, whether in transit or at rest, leaves enterprises vulnerable to attack. Still, there are effective security measures that offer robust data protection across endpoints and networks to protect data in both states. As mentioned above, data encryption is one of the most effective data protection methods for data in transit and at rest.

- **Data-at-rest**: Data-at-rest is data that is not actively moving from device to device or network to network, such as data stored on a hard drive, laptop, or flash drive or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data-at-rest is sometimes considered less vulnerable than data-in-transit, attackers often find data-at-rest a more valuable target than data in motion. The risk profile for data-in-transit or data-at-rest depends on the security measures to secure data in either state.
- **Data-in-transit**: Data-in-transit, or data in motion, is data actively moving from one location to another, such as across the Internet or through a private network. Data protection in transit protects this data while it travels from network to network or is transferred from a local storage device to a cloud storage device. Wherever data is moving, effective data protection measures for in-transit data are critical, as data is often considered less secure while in motion.
- **Data-in-use**: Compromising data in use enables access to data that may have been encrypted at rest and/or in motion. For example, someone with access to random access memory can parse that memory to locate the encryption key for data-at-rest. Once they have obtained that encryption key, they can decrypt encrypted data at rest.

6.5.2. Deciding What to Encrypt

- **Application sessions**: All application user sessions, whether client/server or web-based applications, that access data from a back-end database or other server should be encrypted and provide end-to-end encryption, that is, from workstation to point of

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

data. It is recommended that all data transmissions between the server and the workstation occur over a VPN that employs FIPS 140-2 compliant end-to-end encryption. If a VPN solution is not feasible, an alternate end-to-end encryption mechanism, such as HTTPS protocol and SSLv3 (TLS) encryption, is acceptable. SSL encryption should be based on a certificate containing a key of no less than 2048 bits.

- **Attachments and removable storage stored files**: Apply file-level encryption to protect data in files attached to emails or stored on removable storage such as flash disks.
- **Backup media**: Tape and hard drive backups require encryption when sensitive data is stored. There are two basic types: host-based encryption, which encrypts the data backed up as it is, and appliance-based encryption devices that store data securely.
- **Classified, sensitive, or personally identifiable information (PII)**: Data considered classified, sensitive, or personally identifiable may be required by law, regulation, or contractual obligation, to be encrypted and may be subject to data breach notification requirements.
- **Cloud computing**: Cloud storage providers offer encryption services to encrypt data before it is transferred to the cloud for storage. Typical cloud encryption applications range from encrypted connections to limited encryption only of data that is known to be sensitive (such as account credentials) to end-to-end encryption of any data that is uploaded to the cloud. In these models, cloud storage providers encrypt data upon receipt, passing encryption keys to the customers to safely decrypt data when needed.
- **Mobile devices**: Apply full hard drive encryption to protect data stored on mobile devices. If they do not have the username and password, they cannot access the data on it. They cannot boot it. They cannot even access the files if they remove the hard drive and try to mount it from another system.

r1ne01.ir

6.5.3. Determining Encryption Requirements

The following should be considered when determining encryption requirements:

- **Technical requirements**: Encryption is technology-dependent, and not all encryption technologies may be appropriate. Managing encryption keys can be problematic if a process is not in place. Losing a key, for example, can lead to the inability to access data. The overhead to encrypt and decrypt should also be considered from a performance perspective.
- **Regulatory requirements**: Many legal and regulatory statutes worldwide require data encryption to protect confidential and sensitive information. In some cases, the legislation even prescribes specific encryption controls that must be deployed and what and how data is to be encrypted.
- **Policy requirements**: Encryption is an effective policy enforcement mechanism and should be named within data protection policies. CISOs need to ensure policies match the encryption strategy.
- **Data classification requirements**: A classification schema is required if an organization wants to encrypt its most critical information. This limits the amount of encryption needed and keys to be managed.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following matrix presents the differences between some of the most used encryption algorithms:

Factor	DES	3-DES	AES	Blowfish
Key Length	56	112, 168	128, 192, 256	32 - 448
Developed	1975	1978	1998	1993
Cipher Type	Symmetric	Symmetric	Symmetric	Symmetric
Security	Poor	Good	Better	Best
Potential Keys	2^{56}	2^{112}	2^{128}	Unlimited with Subkeys
Speed	Fast	Slow	Medium	Fast
Brute Force Attack	<1 Day	$1.6x10^{14}$	10^{19}	Unknown
Attacks	Brute Force	Theoretically Possible	Side Channel	Birthday

Table 23: Encryption Standard Comparison

6.5.4. Selecting, Integrating, and Managing Encryption Technologies

To assist in making the right decisions in establishing an encryption strategy, NIST has published NIST SP 800-53 Rev. 5 that provides a set of encryption controls:

- **IA-7: Cryptographic module authentication:** The information system uses mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.
- **SC-8: Transmission confidentiality and integrity:** The information system protects the data's integrity and confidentiality.
- **SC-12: Cryptographic key establishment and management:** When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.
- **SC-13: Cryptographic protection:** Cryptography can be applied in different use cases to support a variety of security solutions. It must be implemented in accordance with applicable laws, directives, regulations, guidelines, etc.
- **SC-17: Public Key Infrastructure certificates:** In cryptographic systems with a hierarchical structure, a trust anchor is the authoritative source (e.g., a certificate authority) for which trust is assumed and not derived and is used to validate and verify the authenticity of a certificate.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. VIRTUALIZATION SECURITY

Virtualization security is the methods and practices that are used to protect an IT infrastructure that has been virtualized in whole or part. Addressing the unique risks of virtualized devices goes beyond existing information security controls as they are designed to protect physical hardware consisting of servers, endpoint devices, storage, and networks. The concepts are the same; for example, configuration and patching of assets are similar; however, how you apply these controls is different. Virtualization is a foundational technology for cloud computing; subsequently, CISOs will invariably need to apply security to virtual assets and resources. Before attempting to secure a virtualized infrastructure, you should have a basic understanding of virtualization.

7.1. Virtualization Overview

Today, CISOs more often deal with virtual rather than actual computing environments where many (virtual) versions of operating systems, storage devices, or networking resources will exist on a single or multiple-meshed physical device infrastructure. Creating a software-based or virtual representation of a computing environment is one of the most effective ways to reduce IT expenses. Multiple virtual machines (VMs) can be deployed on a single physical machine. Hypervisors control these VMs by dynamically allocating the material resources of the host. VMware's vSphere and Microsoft's Hyper-V products are the two most used virtual software environments a CISO will typically be exposed to.

The following model is a representation of a virtualized environment:

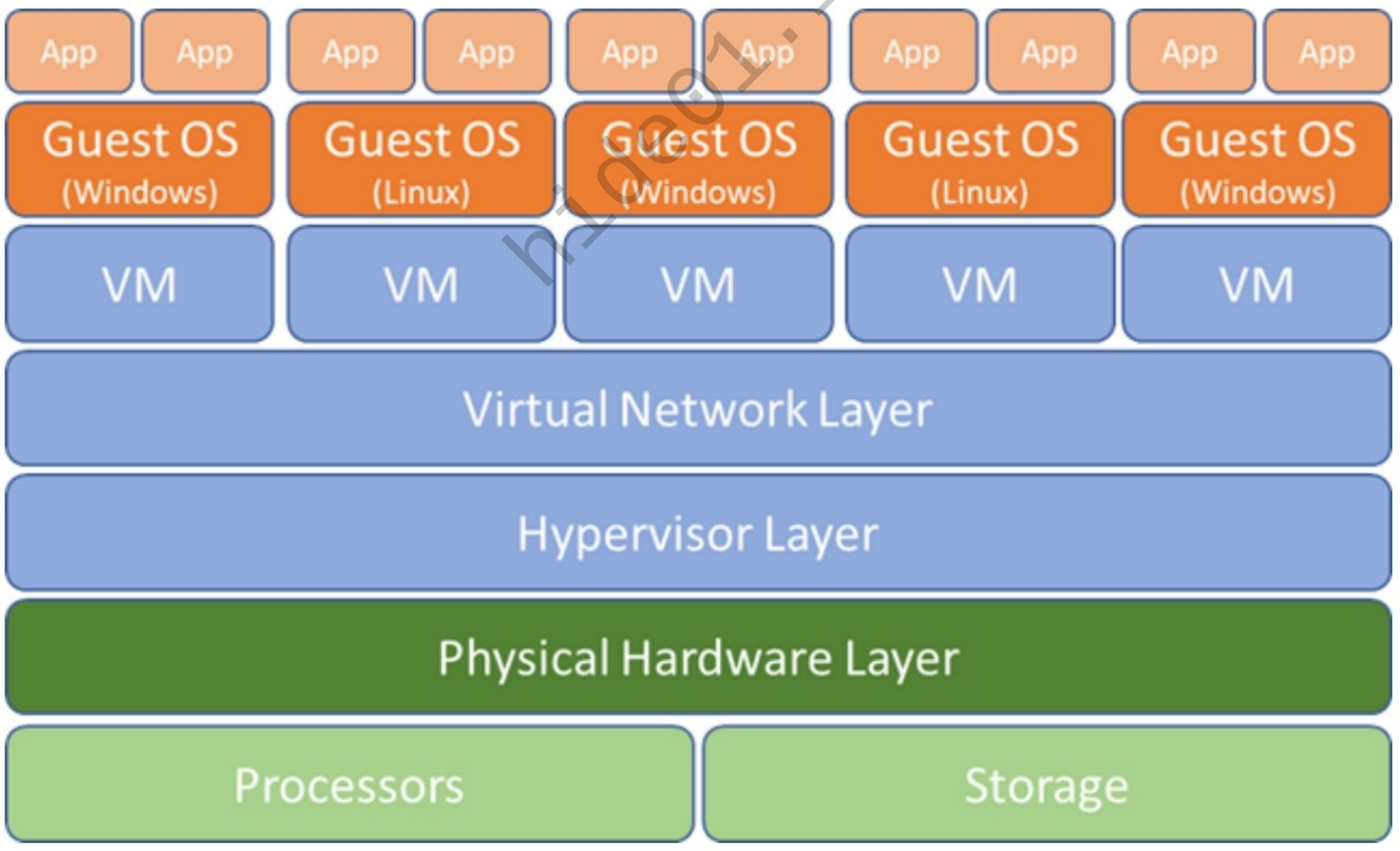


Figure 55: Virtualized Environment

To understand the risks of a virtualized environment, you will need to understand the basic types of virtualizations that exist:

- **Desktop virtualization**: The separation of the desktop environment and associated application software from the physical client device that is used to access it.
- **Full virtualization**: A virtualization technique that is a complete simulation of the underlying hardware.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network virtualization**: Process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network.
- **Operating system virtualization (containerization)**: The existence of multiple isolated user-space instances referred to as containers or partitions that look like real computers from the point of view of programs running in them.
- **Paravirtualization**: Is a virtualization technique that presents a software interface to the virtual machines which is similar, yet not identical, to the underlying hardware–software interface.
- **Storage virtualization**: The virtualization of storage to enable better functionality and more advanced features in computer data storage systems.

7.2. Virtualization Risks

Due in significant part to the fact that cloud computing is so inexorably linked to virtualization, the Cloud Security Alliance (CSA) created a working group to identify risks and controls specific to virtual infrastructures.

The following are the top core risks developed by CSA's Virtualization Working Group:

Risk	Summary
1) VM sprawl	The uncontrolled proliferation of VMs can lead to an unmanageable condition of unpatched and unaccounted-for machines.
2) Sensitive data within a VM	Data confidentiality within VMs can be compromised because data can be easily transported and tampered with.
3) Security of offline and dormant VMs	Dormant and offline VMs can eventually deviate so far from a current security baseline that simply powering them on introduces extensive security vulnerabilities.
4) Security of preconfigured (golden image) VM/active VMs	VMs exist as files on a virtualization platform, which can lead to unauthorized access, resulting in machine configuration changes or viral payload injection into the platform's virtual disks.
5) Lack of visibility into and control over virtual networks	Software-defined virtual networks can cause network security breaches because traffic over virtual networks may not be visible to security protection devices on the physical network.
6) Resource exhaustion	Uncontrolled physical resource consumption by virtual processes can lead to reduced availability.
7) Hypervisor security	Uncontrolled physical resource consumption by virtual processes can lead to reduced availability.
8) Unauthorized access to hypervisor	Administrative access controls to the hypervisor may not be adequate to protect against potential attacks.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Risk	Summary
9) Account or service hijacking through the self-service portal	Portal vulnerabilities can lead to privilege escalation attacks.
10) Workloads of different trust levels located on the same server	Ensure that there is sufficient security segregation of workloads on a physical host.
11) Risk due to cloud service provider API	A hybrid (private/public) cloud virtualization implementation can pose security risks due to account/authentication federation.

Table 24: CSA Core Virtualization Risks

7.3. Virtualization Security Concerns

The primary risks to a virtualized environment begin with the fact that virtualization adds additional layers of complexity. Not only does a CISO need to be concerned with the threat inherent to the physical host environment but also the virtualized technology. For example, VMs are dynamically deployed, creating a phenomenon called virtual sprawl. This is where organizations lose track of their VMs and what is and is not patched, creating a situation where the integrity of a virtualized instance, or even the overall environment, can no longer be assured.

Protecting a virtualized environment has some unique aspects compared to protecting a physical environment and requires a separate but integrated approach to information security. Virtualization security covers a broad spectrum of methods to protect information and assets.

Some of the issues CISOs face in securing their virtualized infrastructure include:

- Ensuring that cyberattacks beginning at the physical host do not permeate the virtualized environment.
- Tracking and monitoring VMs on and offline to identify and monitor virtual assets.
- Implementing security controls granularly for each VM.
- Ensuring control and authority over each VM to prevent unauthorized access.
- Deploying security policies across the virtualized infrastructure.
- Implementing security solutions (antimalware, firewalls, IPS etc.) specifically designed to protect a virtualized environment.
- Ensuring security patches are applied to both online and offline VMs.

7.4. Virtualization Security Controls

NIST has led the security industry in the identification of adequate security controls for virtualized environments. Through a series of publications, NIST provides guidance on how organizations can address the threats and vulnerabilities inherent to a virtualized environment.

The following presents the family of NIST SPs oriented to protecting a virtualized environment:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 56: NIST SP Virtualization Protection Guidance

SP 800-125 (2011) / Guide to Security for Full Virtualization Technologies [55]

Abstract: SP 800-125 aims to discuss the security concerns associated with full virtualization technologies for server and desktop virtualization and to provide recommendations for addressing these concerns. Full virtualization technologies run one or more operating systems and their applications on top of virtual hardware. Full virtualization is used for operational efficiency, such as in cloud computing, and for allowing users to run applications for multiple operating systems on a single computer.

SP 800-125A Rev. 1 (2018) / Security Recommendations for Hypervisor Deployment on Servers [99]

Abstract: The hypervisor is a collection of software modules that provides virtualization of hardware resources (such as CPU/GPU, memory, network, and storage) and thus enables multiple computing stacks (made of an operating system and application programs) called virtual machines (VMs) to be run on a single physical host. Also, it may have the functionality to define a network within the single physical host (called virtual network) to enable communication among the VMs resident on that host as well as with physical machines and VMs outside the host. With all this functionality, the hypervisor is responsible for mediating access to material resources, providing runtime isolation among resident (guest) VMs, and enabling a virtual network that provides security-preserving communication flow among the VMs and between the VMs and the external network. The architecture of a hypervisor can be classified in separate ways. The security recommendations in this document relate to ensuring the secure execution of baseline functions of the hypervisor and are, therefore, agnostic to the hypervisor architecture. Further, the recommendations are in the context of a hypervisor deployed for server virtualization and not for other use cases such as embedded systems and desktops.

SP 800-125B (2016) / Secure Virtual Network Configuration for Virtual Machine (VM) Protection [100]

Abstract: Virtual machines (VMs) are vital resources to be protected because they are the computer engines hosting mission-critical applications. Because VMs are end nodes of a virtual network, the configuration of the virtual network is an essential element in the security of the VMs and their hosted applications. The virtual network configuration areas discussed in this document are network segmentation, network path redundancy, traffic control using firewalls, and VM traffic monitoring. This document analyzes the configuration options under these areas and presents recommendations for secure virtual network configuration for VM protection.

7.5. Virtualization Security Reference Model

Once you have selected the proper set of controls to protect your organization's virtualized environment, you can apply them according to a reference model to ensure controls are correctly deployed. The virtualized reference model is an abstract view of where security controls should

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

be applied to a virtualized environment:

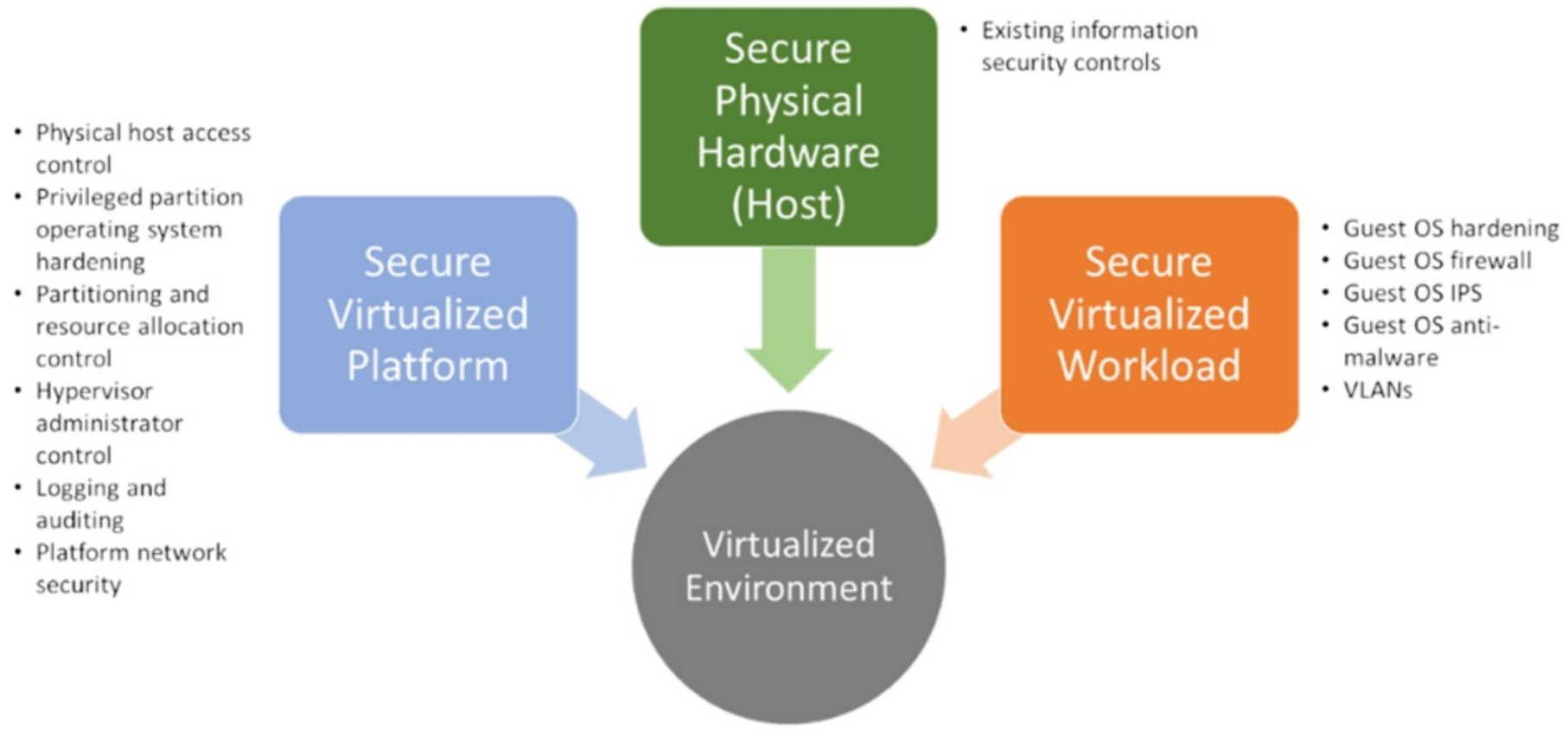


Figure 57: Virtualized Security Reference Model

8. CLOUD COMPUTING SECURITY

Cloud computing security is the methods, practices, and solutions that protect an organization's in-house, external, or hybrid cloud computing environment. Virtually every organization today uses some form of cloud computing; subsequently, CISOs must be savvy in protecting information processed in the cloud. Ironically, despite the high adoption rate of cloud computing, many organizations do not have a high degree of trust in placing their applications and data in the cloud. On April 23, 2017, a Forbes article on the State of Cloud Adoption and Security stated that just 23% of organizations today trust entirely public clouds to keep their data secure [101]. As the CISO of your organization, one of your jobs will be to instill user confidence in cloud computing to enable its further adoption which is inevitably a request of the business and/or technology department. Before attempting to secure a cloud computing infrastructure, you should have a basic understanding of what cloud computing is.

8.1. Overview of Cloud Computing

Cloud computing is the delivery of computing services over the Internet. Computing services consist of server processing, data storage, applications/databases, network services, software, and anything else that can be delivered over the Internet. Reduced cost, increased speed, more agility, unlimited scale, high reliability, and improved productivity are the main reasons organizations have moved their in-house applications and processes to cloud service providers or even developed their own in-house cloud infrastructure.

Over time, several types of cloud computing have emerged:

- **Public cloud**: Public clouds are owned and operated by a third-party cloud service provider, which delivers computing resources like servers and storage over the Internet. Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), are examples of public clouds. With a public cloud, the cloud provider owns and manages all hardware, software, and other supporting infrastructure. You access these services and manage your account using a web browser.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Private cloud**: A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located in the company's on-site data center. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.
- **Community cloud**: A community cloud is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, and so on), whether managed internally or by a third party and hosted internally or externally. This type of cloud is controlled and used by a group of organizations.
- **Hybrid cloud**: A combined public and private cloud, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, the hybrid cloud gives businesses greater flexibility and deployment options.

The following summarizes the cloud computing types:

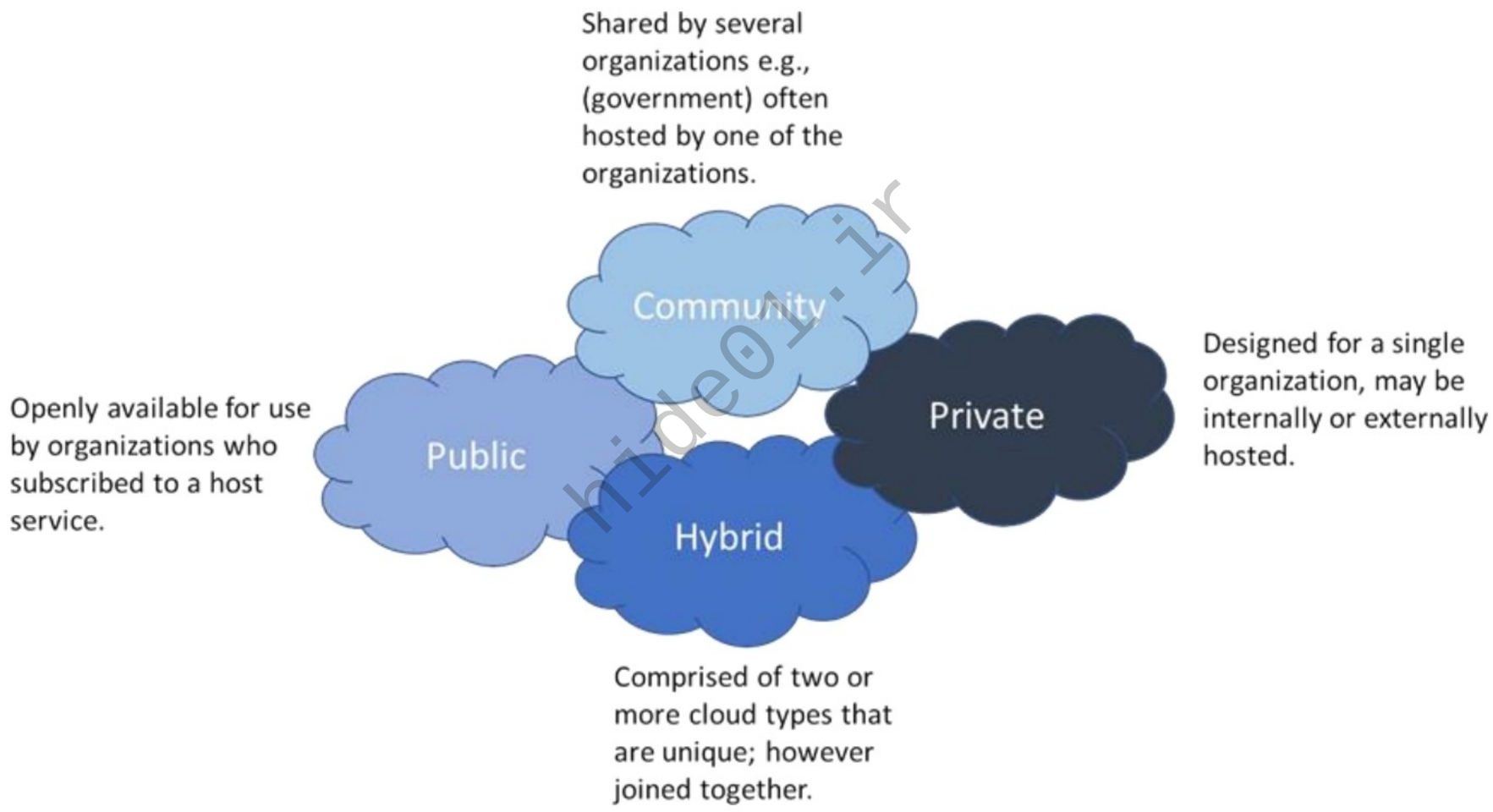


Figure 58: Cloud Computing Types

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). These are sometimes called cloud computing stacks because they build on top of one another. Knowing what they are and how they differ makes it easier to accomplish your business goals.

- **IaaS**: The most basic category of cloud computing services. With IaaS, you rent IT infrastructure - servers and VMs, storage, networks, operating systems - from a cloud provider on a pay-as-you-go basis.
- **PaaS**: PaaS refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SaaS**: SaaS is a method for delivering software applications over the Internet, on-demand, and typically on a subscription basis. With SaaS, cloud providers manage the software application and underlying infrastructure and any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet, or PC.

Cloud computing services all work differently, depending on the provider. However, many provide a friendly, browser-based dashboard that makes it easier for IT professionals and developers to order resources and manage their accounts. Some cloud computing services are designed to work with REST APIs and a command-line interface, giving developers multiple options.

8.2. Security and Resiliency Cloud Services

With the wide adoption of cloud computing came the emergence of specialized cloud services for information security and disaster recovery. As a CISO, you must compare these specialized cloud computing services to similar services provided by your IS organization. The following are the prime categories:

- **Security as a service (SECaaS)**: A business model in which a service provider integrates their security services into a corporate infrastructure on a subscription basis more cost-effectively than most individuals or corporations can provide when the total cost of ownership is considered.
- **Backup as a service (BaaS)**: An approach to backing up data that involves purchasing backup and recovery services from an online data backup provider.
- **Disaster recovery as a service (DRaaS)**: A cloud computing and backup service model that uses cloud resources to protect applications and data from disruption caused by disaster. It gives an organization a total system backup for business continuity during system failure.

hide01.ir

8.3. Cloud Security Concerns

The CSA dives into all cloud security issues and threats. Through its research, it isolated the most significant threats affecting cloud computing. Here, we briefly summarize the cloud security issues listed in the "The Treacherous 12 – Top Threats to Cloud Computing [102]" report, along with other vital terms cybersecurity professionals need to know.

- **Data breach:** One of the foremost concerns and issues affecting all the ways of computing, including cloud computing. A data breach is when a hacker successfully taps into a network and collects sensitive information, such as passwords, health information, financial information, trade secrets, and intellectual property.
- **Poor identity and sign-in management:** Nonsecure sign-ins and weak passwords enable hackers to access devices and networks. The best advice is to use encrypted passwords, rotate passwords, cryptographic keys, and certificates, and employ a multi-factor authentication protocol to grant account access.
- **Nonsecure APIs and interfaces:** APIs and UIs are like pawns on a chessboard regarding cloud security defense. Cloud service providers reveal these interfaces for cloud computing users to interact with the cloud, which places APIs and UPIs on the front line of attack.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CSA warns that APIs and UIs require heightened and robust security because they are the first level a hacker will try to breach.

- **System vulnerabilities:** Attacks via system vulnerabilities are not new and have existed since at least the invention of networking. Vulnerabilities occur when hackers use available bugs to penetrate a computing device. After accessing the device via a bug, hackers may steal information, control the machine, or disrupt operations.
- **Account hijacking:** Phishing, fraud, and taking advantage of bugs are ways to hijack accounts. These are not novel methods for hackers. However, a new threat is presented when it comes to cloud security issues. After gaining access to sign-in information, Hackers may spy on cloud computing activities, including search history and transactions, and they can manipulate data, create false information, and direct users to non-credible websites. CSA advises not sharing passwords with multiple organization users and incorporating multi-factor authentication.
- **Malicious insiders:** A current or former employee who has/had access to sensitive information might use their access for nefarious purposes. For example, an administrator responsible for performing regular backups of the systems where client resources are hosted (VMs, data stores) could exploit the fact that they have access to backups and thus exfiltrate sensitive user data.
- **Advanced persistent threat (APT):** This long-term game of attack takes hackers time to execute. The goal is often to penetrate an enterprise's computing infrastructure to collect trade secrets and intellectual property or maintain access for future use. Hackers will adapt their methods to breach the various infrastructure components as they encounter the various network security protections that are in place.
- **Data loss:** The permanent loss of data, which may occur for cloud services during a natural disaster (fire, earthquake, etc.) or when a cloud service provider (CSP) unintentionally erases data. The best course of action is to back up data in case of a data loss scenario.
- **Insufficient due diligence:** When an enterprise switches to a cloud service, it must comprehensively review the process and implement a thorough roadmap to move its services to the cloud. A lack of preparation and forethought opens the company to security vulnerabilities.
- **Abuse and nefarious use of cloud services:** Cloud computing is vulnerable to attack when proper security measures are not in place before deployment, often for free trials and fake account sign-ups that use a payment method. The CSA report cites these examples of misuse, "launching DDoS attacks, email spam, and phishing campaigns; mining for digital currency; large-scale automated click fraud; brute-force compute attacks of stolen credential databases; and hosting malicious or pirated content."
- **Denial-of-service:** Denial-of-service (DoS) describes attacks that prevent users from accessing their information and applications. This method of attack uses system resources, such as power, memory, and hard drive space, in abundance to slow down the system enough that users cannot access their information.
- **Shared technology vulnerabilities:** Off-the-shelf hardware and software components help make up a cloud infrastructure and are a shared resource. Its security is vulnerable

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

when isolation properties are not incorporated into the infrastructure that provides the cloud deployment capabilities. One vulnerability in the cloud infrastructure may lead to the entire cloud service provider's environment being compromised.

8.4. Cloud Security Controls

The leading authority on cloud computing security controls is CSA. Founded in 2008, CSA is an international member-driven organization chartered with promoting best practices for providing security assurance within cloud computing. CSA certifies cloud security practitioners, publishes the Cloud Control Matrix (CCM), and maintains a registry of trusted cloud service providers [103].

In 2010, the CSA released the CCM as a uniform set of controls to measure the security readiness of cloud-centric security programs. CCM is cross mapped to dozens of other security controls, including COBIT, ISO 27001, HIPAA/HITECH [26], PCI DSS, etc. CCM includes 133 controls organized by 16 domains.

The following is a breakdown of the CCM controls:

	Domain	Controls
AIS	Application & Interface Security	4
AAC	Audit Assurance & Compliance	3
BCR	Business Continuity Mgt & Ops Resilience	11
CCC	Change Control & Config. Management	5
DSI	Data Security & Information Lifecycle Mgt.	7
DSC	Datacenter Security	9
EKM	Encryption & Key Management	4
GRM	Governance & Risk Management	11
HRS	Human Resources Security	11
IAM	Identity & Access Management	13
IVS	Infrastructure & Virtualization	13
IPY	Interoperability & Portability	5
MOS	Mobile Security	20
SEF	Sec. Incident Mgt., E-Discovery & Cloud Forensics	5
STA	Supply Chain Mgt. Transparency & Accountability	9
TVM	Threat & Vulnerability Management	3

Table 25: CCM Controls Matrix

8.5. Cloud Computing Protection Considerations [104]

The following covers unique security considerations that CISOs should address within their cloud computing environment, whether in-house or provided by a third party:

- **Cloud access security broker (CASB)**: A cloud service provider must allow legitimate network traffic and block malicious network traffic, just as any other Internet-connected organization does. However, unlike traditional IT service organizations, a CSP will not necessarily know what network traffic its customers plan to send and receive. A CASB acts as a gatekeeper, allowing the organization to extend the reach of its security policies beyond its infrastructure.
- **Cloud application security**: Application security poses specific challenges to the cloud service provider and the customer. Organizations must apply the same diligence to application security as physical and infrastructure security. If an application is

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

compromised, it can create financial liability and reputational damage to both the provider and the customer, especially if the ultimate end users of the application are customers of the cloud service customer rather than its employees. Understanding the application security policy considerations based on the different cloud deployment models is essential to protect an application from data breaches.

The following points highlight the impact of cloud deployment models on application security.

- **IaaS**: The customer has responsibility for the deployment of the complete software stack - operating system, middleware, and application - and for all aspects of security that relate to this stack, including the application of all appropriate security patches. The application security policy should closely mimic the policy of applications hosted internally by the customer. Also, it should consider inclusion in security operations that may be required due to the cloud services shared responsibility model.
- **PaaS**: The customer should identify potential threats and their impacts should they occur, as well as how to respond to the potential threats. They should request regular security reports from their cloud vendor and ensure an understanding of how the data is protected. The customer is responsible for application deployment and securing access to the application itself. The provider is responsible for adequately ensuring the infrastructure, operating system, and middleware.
- **SaaS**: Application-tier security policy controls are mostly the provider's responsibility and depend upon terms in the contract and service level agreement (SLA). The customer must ensure that these terms meet their confidentiality, integrity, and availability requirements. Understanding things like the provider's patching schedule, controls against malware, and the release cycle, are essential.
- **Cloud computing auditing**: As a baseline, customers should expect to see a report of the cloud service provider's operations by independent auditors. The level of access to essential audit information is a crucial consideration of contracts and SLA terms with any cloud service provider. As part of any terms, cloud service providers should offer timely access to audit events and log and report information relevant to a customer's specific data or applications.
- **Cloud data protection**: The questions relating to data for cloud computing are about various forms of risk: risk of theft or unauthorized disclosure of data, risk of tampering or unauthorized modification of data, risk of loss or unavailability of data, and risk of keeping data longer than it is needed. In the cloud, "data assets" may also include application programs or machine images, which can present the same risks as the contents of databases or data files.

For IaaS, more responsibility is likely to be with the customer (for example, for encrypting data stored on a cloud storage device).

- PaaS cloud services present unique challenges in sharing responsibility between the customer and provider. Understanding how each service is used within the PaaS environment to manage data security, including encryption, log file handling, and administrative access, is essential. The customer needs to know what obligations it retains and the available features and configuration of the PaaS service that can facilitate data security.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For SaaS, more responsibility is likely to be with the provider because neither the stored data nor the application code is directly visible or controllable by the customer.

- **Cloud identity access control**: The cloud service provider must have a secure system for provisioning and managing unique identities for their users and services. This identity and access management functionality must support simple resource access and robust customer application and service workflows. Any user access to the provider's management platform, regardless of role or entitlement, should be monitored and logged to provide auditing of all access to customer data and applications.
- **Cloud service agreements**: The primary means cloud service customers have to ensure that their applications and data hosted in cloud services are secured following their security and compliance policies is to verify that the cloud service agreement between the customer and the provider, along with associated documents such as the SLA, contain all their requirements. It is vital for the customer to understand all the terms related to security and privacy and to ensure that those terms meet their needs. The agreement also needs to cover exiting the deal.

9. TRANSFORMATIVE TECHNOLOGIES

Transformative technologies are those that have the potential to change or disrupt the information security industry dramatically. IS has seen many technologies come and go, but we are witnessing large-scale investments in next-generation technologies that can be adapted to the IS world. CISOs need to keep abreast of the future of IS technology, evaluating its benefit or impact on their organizations.

hide01.ir

9.1. Artificial Intelligence

Artificial intelligence (AI), specifically generative AI, is coming to the IS world and, in fact, is already here in several applications, including security information and event management (SIEM) solutions. Hardening assets and encasing sensitive data behind firewalls is less effective than it once was as attackers become more sophisticated. The direction of the industry is to focus on the behavior inside the network to discern if it is appropriate. AI can be used to baseline what is normal for an organization and then detect anything outside those boundaries. Organizations are often trying to defend against yesterday's attacks and lack a focus on today's emerging threats. Matching rules and signatures to known threats is how it has always been done. Evidence of this approach failing is the fact that attackers are in a network 200 days before real damage is done [105].

AI currently shows promise in discerning good and bad actors and bots on the network through behavior analysis. AI can be especially useful in identifying an insider attack when it detects a trusted employee with elevated privileges acting in a manner inconsistent with their role. Regardless of the varying opinions on AI, it is highly likely that it is here to stay and will only become more pervasive, first as a component of existing security technology and then as an enterprise security platform.

9.2. Augmented Reality

Augmented reality (AR) is a technology where a computer-generated image is superimposed on a user's view of the natural world, creating a composite view. This technology highly appeals to

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

security operations where the superimposed perspective can be a SOC overlaid onto a data center. This could mean that organizations would no longer need to build physical SOCs but rather build an image of a SOC superimposed over their data center or network. SOC analysts and operators could theoretically live and work remotely from anywhere and, through AR technology, experience a function as if they were working in a physical SOC location, even up to interacting with fellow SOC employees utilizing complementary technology such as video conferencing.

Time will only tell if AR is deployed in SOCs; however, its promise and the potential for cost savings make AR a natural fit for SOCs.

9.3. Autonomous SOC

Autonomous technology refers to machines that act independently of humans to perform tasks that are either too expensive or routine for humans. This technology is, for example, being widely developed in autonomous or self-driving automobiles and trucks and is now beginning to show up in the information security industry. Several companies have received funding and are actively pursuing independent security operations platforms to leverage AI to perform security operations functions.

With advancements in AI, organizations are looking for ways to reduce the number of people it takes to run a SOC, specifically to:

- Analyze threat and vulnerability data to discern risk and act.
- Automatically review security bulletins and patch assets accordingly.
- Monitor devices to detect configuration changes and revert to a secure state.
- Automatically maintain and renew certificates.
- Add, delete, or modify firewall rules dynamically when the network changes.
- Scale logging storage space based on increases in events per second.
- Produce regulatory reports according to a preset schedule.

Several more years of development are required before full SOC autonomy is realized, but the path is set, and CISOs need to be prepared.

9.4. Dynamic Deception

Many CISOs believe that defending against attackers is insufficient and that organizations cannot hide from attacks or avoid the inevitable. CISOs must assume that attackers will gain entry to their network. It is not a matter of if, but, when. To change the playing field, a new strategy has emerged: bait the attackers into a zone of a safe network where organizations can monitor, control, quarantine, or eradicate the threat.

This approach is based on the theory of dynamic behavioral deception, where self-learning or AI creates a dynamically changing faux environment attractive to attackers. This method of baiting hackers is designed to lure an attacker to a replica of an organization's assets and information, leading them away from the real ones. Attackers will follow the path of least resistance; here, a path is left for them to follow to the mirrored assets. The dynamic deception is designed to keep pace with the natural environment to convince attackers this is a legitimate target.

The typical components of this type of security software include a self-learning capability to mirror and profile their environment, deployment of deceptive credentials that match network behavior

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and device types, monitoring and recording of the faux environment to allow playback, and analysis and reconstitution of the deceptive environment after infiltration in order to reset it for the next attack.

Deception technology allows organizations to fight back and no longer maintain a passive approach to hackers waiting for them to attack.

9.5. Software-Defined Cybersecurity

Information security has also joined the software-defined movement, where vendors quickly shift their software-based products and services. These products offer a level of self-awareness to the environment where they are deployed and can be modified to align with the changes in the environment or threat landscape through adjustments in software. These adjustments occur through APIs, where they communicate with their environment. For example, firewalls and IPS's can speak with one another to detect and block malicious traffic. This approach is desirable versus hardware and appliance-based approaches as the enterprise's defenses are a software model providing better control, visibility, and agility. For example, security controls can now dynamically scale with events per second without administrator involvement.

These next-generation security software products use software-defined technology to create a security architecture abstraction layer that automates and orchestrates their behavior. This approach joins disparate security products, allowing them to connect and operate seamlessly at the abstraction layer. This abstract layer of software integrates with a network and calls only those functions of the disparate software products to perform as required by the threat, vulnerability, or risk. Now, vulnerability notification feeds are automatically parsed for relevance, impacts are analyzed through an interrogation with the asset inventory, and security patches are pulled and applied with little to no human intervention [106].

hide01.ir

10. SUMMARY

This domain reviews the core competencies of information security. Access control focuses on the fundamental concepts related to an organization's ability to manage access to its resources. The access control plan defines the procedures and requirements for achieving the objectives described in the organization's access control policy. Authentication establishes the process used by a system to verify the identity of a user, process, or service before granting access. Authorization focuses on permissions granted to authenticated users. Finally, access administration addresses the process of provisioning, reviewing, and removing access granted to people, processes, and systems.

Physical security focuses on physical risk analysis, physical security audits, strategy, and facility design to support the protection of personnel and assets.

Network security focuses on the security of an organization's network communications. Although the CISO rarely leads network design and network management, contributions to network security planning, network management, and network design are essential. The CISO should understand the interactions occurring at each OSI model layer. The CISO should also understand standard network security controls and protocols that protect data and VoIP communications.

Application security focuses on system (e.g. software) and application security. The primary concern is incorporating security into all phases of the SDLC, whether the development supports the creation of an IT system, software, or process. Integrating security into all phases of the SDLC requires

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

understanding the waterfall model and common alternatives (e.g. Agile) that guide the requirements, design, implementation, verification, and maintenance processes for development. Once a solution reaches the maintenance phase, ongoing testing, configuration management, and effective disposal are required to support organizational goals for security. DevOps seeks to combine the development and operations teams to improve efficiency and on-going maintenance among other items.

Encryption reviews the processes, technologies, and tools related to encryption. The most critical concerns are symmetric and asymmetric encryption and the key management considerations associated with each approach. PKI, hashing, and digital signatures are also discussed.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|CISO

hide01.ir

DOMAIN 5

Strategic Planning, Finance, and Vendor Management

EC-Council

Introduction

In this last domain, you will be instructed on the core management disciplines of strategic planning, managing the finances of an information security program, procuring information security products or services, assessing supplier security maturity, and overseeing vendor partnerships. These disciplines are traditionally business administration and management duties, and often new skills for many Chief Information Security Officers (CISOs). It is, therefore, essential to cover each in detail sufficient for a CISO to function as a department manager. Strategic planning will show you how to build a business-integrated information security program by becoming a student of the company and industry. Before a CISO can create a strategic information security plan, they must pass a test. That test is that a CISO must be able to present to an external audience in nontechnical language precisely what their company does and describe the industry it serves. A CISO can only effectively design a strategic plan with this essential business acumen.

Many CISOs do not typically manage the finances of their organization due in large part to their lack of financial management knowledge. Senior management assumes CISOs are technocrats and need to gain basic management skills, to include financial management. For a CISO to change this perception, they must build confidence and credibility with their management by understanding finance and knowing how to effectively manage the budget of the information security program while justifying the return on investment.

Procurement is another management discipline CISOs typically lack experience in (apart from sitting in vendor presentations). CISOs commonly make multimillion-dollar buying decisions but only participate a little in the procurement process, including contract negotiations, financing options, and strategic sourcing. A significant aspect of procurement is issuing a Request for Proposal (RFP); however, many executives are not adept at creating effective RFPs and rely on vendor templates. This domain will show you how the procurement process works, what to include in an RFP, and how to negotiate a contract. CISOs usually engage in a lengthy process for vendor selection through an evidence-based evaluation of vendor products and services, which may include qualitatively and quantitatively vetting vendors in an evaluation and selection committee.

Vendor management is a significant part of a CISO's role, as many information security services are outsourced. A CISO must understand standard vendor management practices to work effectively with third parties.

Knowledge Assumptions

It is assumed that most, if not all, of the disciplines covered in this domain are new to a CISO. Consequently, there is no prior knowledge assumed in this domain.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. STRATEGIC PLANNING

Strategic planning is a business management discipline focusing on the systematic processes of envisioning a desired future and defining processes to transform that vision into reality. Strategic planning begins with the desired target state and works backward to the current state to determine the steps and milestones required to achieve the strategic goal.

From the CISO's perspective, the strategic plan must be clearly understood, especially the organization's information security and risk management goals as they relate to the plan. With this understanding, the CISO can outline the roadmap and sequence of progressive and interrelated activities required to achieve the security program's goals. Success depends on the CISO's participation in strategic planning for the organization, the maturity of the organization, and the effectiveness of the governance activities supporting the organization. In addition, risk management and operational goals for the CISO will help refine the details required to develop an effective strategic plan for information security management.

Formulating strategy and defining goals for information security should be closely aligned with the overall corporate business strategic goals and objectives for sustainable organizational success.

- **The Value of Strategic Planning** [107]: According to the Association for Strategic Planning (ASP), highly successful organizations report that strategic planning significantly impacts overall organizational success. Low-success organizations need to report strategic planning as key to overall organizational success.

  From this perspective, the commitment to strategic planning has considerable influence on the success of the information security program. The CISO can develop and mature strategic planning efforts within the information security program regardless of the dedication to this effort in the rest of the organization. Because strategic planning is goal-oriented, the effort to understand the goals of the security program and the steps required to achieve those goals is valuable.

- **Understanding Strategic Planning** [108]: Strategic planning determines goals for the next year or more, how the organization will achieve them, and how it will know if it has been successful. Various perspectives, models, and approaches are used in strategic planning.

- **Goal-based planning** is the most common method and starts with a focus on the organization's mission. It includes reviewing the organization's vision and values, goals to work toward the mission, strategies to achieve the objectives, and action planning (who will do what and by when).

- **Issues-based strategic planning** often starts by examining issues within the organization, strategies to address those issues with action plans.

- **Organic strategic planning** might start by articulating the organization's vision and values and then creating action plans to achieve the vision while adhering to those values.

A strategic plan is developed based on the nature of the organization's leadership, the organization's culture, the complexity of the organization's environment, the organization's size, and the expertise of planners.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.1. Understanding the Organization

Understanding how your organization is structured and operates as a business was covered in Domain 1; however, an additional level of detail is required before creating a strategic plan. CISOs must develop an in-depth understanding of their organization to build the right portfolio of information security services and capabilities for the program-desired goals and objectives. The CISO's journey to becoming a student of their organization and industry includes understanding their organization's dynamics, motivations, and culture. This is essential to ensuring the information security program appropriately interacts with the organization. It is also necessary to understand an organization's maturity level to provide insight into the expected level of maturity an information security program should achieve.

Understanding an organization helps identify the boundaries within which the information security program should exist. CISOs must work within these boundaries to effectively create a security culture, interact with stakeholders, and know how their information security program can be funded and how to monitor and measure its success.

1.1.1. Understanding the Business Structure

The journey of organizational understanding begins with learning how an organization is structured. There are four common organizational structures a CISO is likely to work within:

- **General Corporation:** Also known as a C corporation, this is the most common corporate structure. C corporations can have an unlimited number of stockholders. Consequently, this structure is usually chosen by those companies planning to have more than 30 stockholders or extensive public stock offerings. Since a corporation is a separate legal entity, a stockholder's liability is usually limited to the amount of investment in the corporation and no more. C corporations are also taxed separately from their owners.
- **Close Corporation:** This structure is most appropriate for the individual starting a company alone (a sole proprietorship) or with a small number of people (a partnership). A few significant differences exist between a general corporation and a close corporation. A close corporation limits stockholders to a maximum of 30. In addition, many close corporation statutes require that the directors of a close corporation must first offer the shares to existing stockholders before selling to new stockholders. Closed corporations are not allowed to have a public offering of their shares. Not all local or national governments recognize close corporations.
- **Subchapter S Corporation:** This general corporation limited to the U.S. has elected a special tax status with the Internal Revenue Service (IRS), a federal agency in the U.S., after the corporation has been formed. All owners must be U.S. citizens. Subchapter S corporations are most appropriate for small-business owners and entrepreneurs who prefer to be taxed as if they were still sole proprietors or partners. When a general corporation makes a profit, it pays a federal corporate income tax. If the company also declares a dividend, the stockholders must report the dividend as personal income and pay more taxes.
- **Limited Liability Company (LLC):** While this is not a corporation, it offers many of the same advantages. Many small-business owners and entrepreneurs prefer LLCs because they combine the limited liability protection of a corporation with the *pass-through* taxation of a sole proprietorship or partnership. LLCs have additional

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

advantages over corporations. The two most significant advantages are that they allow greater flexibility in management and business organization, and they do not have the ownership restrictions of S Corporations, making them ideal business structures for foreign investors.

1.1.2. Determining and Aligning Business and Information Security Goals

Their goals must be aligned for an information security program to be coordinated with an organization. This alignment creates a relationship where the business and the information security department can achieve their goals without impacting one another. Aligning the information security program with the company's goals makes the program an integral part of the business, increasing its value proposition.

However, before you can align your information security program with your organization's vision, you need a clear picture of the organization's business goals. The good news is that this is already likely done. As the CISO for your organization, you have the responsibility to find those goals, which exist in strategic plans, marketing collaterals, annual reports, shareholders presentations, published websites, or in employee training materials.

The following matrix provides an example of how CISOs can align business and information security goals:

Business Goal	Information Security Program Goal
1. Reduce risk to the business.	Manage or mitigate operational risk that could impact critical business functions.
2. Comply with all industry legal and regulatory compliance statutes.	Implement information security controls to ensure compliance with legal and regulatory requirements.
3. Provide customers with an effortless buying experience.	Provide secure and seamless online customer transactions.
4. Lead competition through first to market advantage of new products.	Leverage security as an enabler to reduce time to market.
5. Maintain a disciplined approach to spending and investment.	Deploy automation to reduce the manual cost of securing assets and information.

hidegl.ir

Table 26: Business to Information Security Goals Alignment Example

Goal-based strategic planning is often the best way to develop an information security plan because the CISO's primary goal is aligning the information security strategy with the organization's business strategy.

1.1.3. Identifying Key Sponsors, Stakeholders, and Influencers

There are three roles that CISOs must understand and interact with to build support for their information security program. At the highest level is a sponsor. A sponsor is someone who can make or break the program, and they benefit directly from it. They typically authorize or fund information security programs.

While stakeholders have some influence over outcomes, their influence is limited compared

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

with that of sponsors. A stakeholder is anyone who has an interest in the outcome of the information security program. It is essential to understand the stakeholders of a project and how they influence the project's outcome. It is necessary to identify and understand both positive stakeholders who contribute to the program and negative stakeholders who resist or hinder the program.

Influencers are those within the organization with a respected opinion. They can be instrumental in promoting various information security program initiatives. For example, if a critical network administrator is not consulted on a proposed network security technology, their lack of involvement or support could be echoed by others who feel a decision was made in a vacuum without consulting the right people.

The following summarizes the relative importance of the three roles:

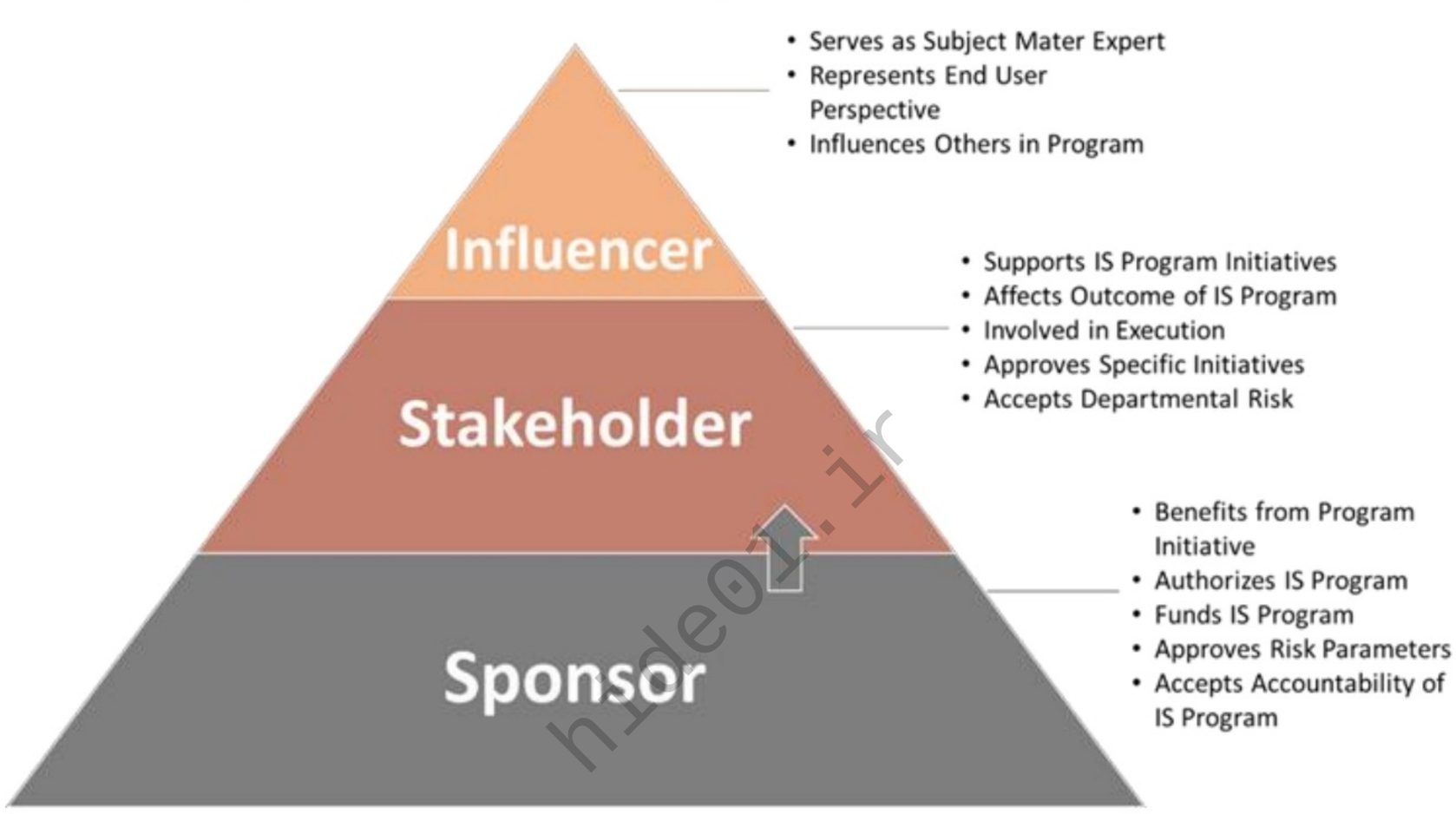


Figure 59: Information Security Program Support Pyramid

1.1.4. Understanding Organizational Financials

Effective CISOs understand the finances of their organization. They can converse equally with senior management and business unit managers concerning finance. Doing this requires understanding the basics of finance and how to read your organization's financial statements. Knowing how your company makes, borrows, and spends money to support ongoing operations and what is left afterward is essential to becoming an effective manager in today's organization.

The following section is excerpted from the U.S. Securities and Exchange Commission—Beginner's Guide to Financial Statement [109].

There are four main financial statements: (1) balance sheets, (2) income statements, (3) cash flow statements, and (4) statements of shareholders' equity. Balance sheets show what a company owns and owes at a fixed point in time. Income statements show how much money a company makes and spends. Cash flow statements show money exchange between a company and the outside world over a period. The fourth financial statement, called a *statement of shareholders' equity*, shows changes in the interests of the company's shareholders over time.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Following is a discussion of the first three financial statements in more detail.

Balance Sheets

A balance sheet provides detailed information about a company's assets, liabilities, and shareholders' equity.

- **Assets:** Assets are things that a company owns that have value. This typically means they can either be sold or used by the company to make products or provide services that can be sold. Assets include physical property, such as plants, trucks, equipment, and inventory. They also include things that cannot be touched but exist and have value, such as trademarks and patents. And cash itself is an asset, as well as the company's investments.
- **Liabilities:** Liabilities are money that a company owes to others. This can include all kinds of obligations, like money borrowed from a bank to launch a new product, rent for the use of a building, money owed to suppliers for materials, payroll a company owes to its employees, environmental cleanup costs, or taxes owed to the government. Liabilities also include obligations to provide future goods or services to customers.
- **Shareholder Equity:** Capital or net worth is the money left if a company sells all its assets and pays off all its liabilities. This leftover money belongs to the company's shareholders or the owners.

Income Statements

An income statement is a report that shows how much revenue a company earned over a specific time (usually for a year or some portion of a year). An income statement also shows the costs and expenses of gaining that revenue. The literal *bottom line* of the statement usually shows the company's net earnings or losses. This tells you how much the company earned or lost over the period.

hidoc1.ir

Income statements also report Earnings Per Share (EPS). This calculation tells you how much money shareholders would receive if the company distributed all the net earnings for the period.

Cash Flow Statements

Cash flow statements report a company's inflows and outflows of cash. This is important because a company must have enough cash to pay its expenses and purchase assets. While an income statement can tell you whether a company made a profit, a cash flow statement can tell you whether the company generated cash.

A cash flow statement shows changes over time rather than absolute dollar amounts at a point in time. It uses and reorders the information from a company's balance sheet and income statement.

The bottom line of the cash flow statement shows the net increase or decrease in cash for the period. Cash flow statements are divided into three main parts. Each part reviews the cash flow from one of three activities: (1) operating, investing, and (3) financing activities.

- **Operating Activities:** The first part of a cash flow statement analyzes a company's cash flow from net income or losses. For most companies, this section of the cash flow statement reconciles the net income (as shown on the income statement) to the actual cash the company received from or used in its operating activities. To do this,

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

it adjusts net income for any noncash items (such as adding back depreciation expenses). It changes for any cash used or provided by other operating assets and liabilities.

- **Investing Activities:** The second part of a cash flow statement shows the cash flow from all investing activities. This includes purchases or sales of long-term assets, such as property, plant, equipment, and investment securities. If a company buys a piece of machinery, the cash flow statement would reflect this activity as a cash outflow from investing activities because it used cash. If the company decided to sell off some investments from an investment portfolio, the proceeds from the sales would show up as a cash inflow from investing activities because it provided cash.
- **Financing Activities:** The third part of a cash flow statement shows the cash flow from all financing activities. Typical cash flow sources include cash raised by selling stocks and bonds or borrowing from banks. Likewise, paying back a bank loan would show up as a use of cash flow.

A positive cash flow indicates that a company's liquid assets are increasing. A positive cash flow means more cash is coming in than going out, which is essential for a business to sustain long-term growth. A company can report profits (positive earnings) on its income statement but still go out of business or struggle to attract investors. As such, operating a positive cash flow is often viewed as a better ongoing measure of a company's financial health. The statement of cash flows is the only financial statement that is hard to manipulate.

1.2. Creating an Information Security Strategic Plan

A CISO's most important responsibility is creating an information security strategy that aligns with organizational business goals. A CISO must understand their organization's industry, business model, growth trajectory, risk appetite, and asset protection needs. A strategy defines how CISOs leverage an information security program to secure information and assets. However, a documented program strategy still needs to be completed for many organizations. A 2018 survey conducted by Educause revealed only 30 percent of those surveyed had a documented security strategy [110].

A leading factor for the lack of security program strategies is an equal lack of understanding of just what constitutes a strategy. The following framework should help to guide the development of a strategic information security plan.

hideoir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

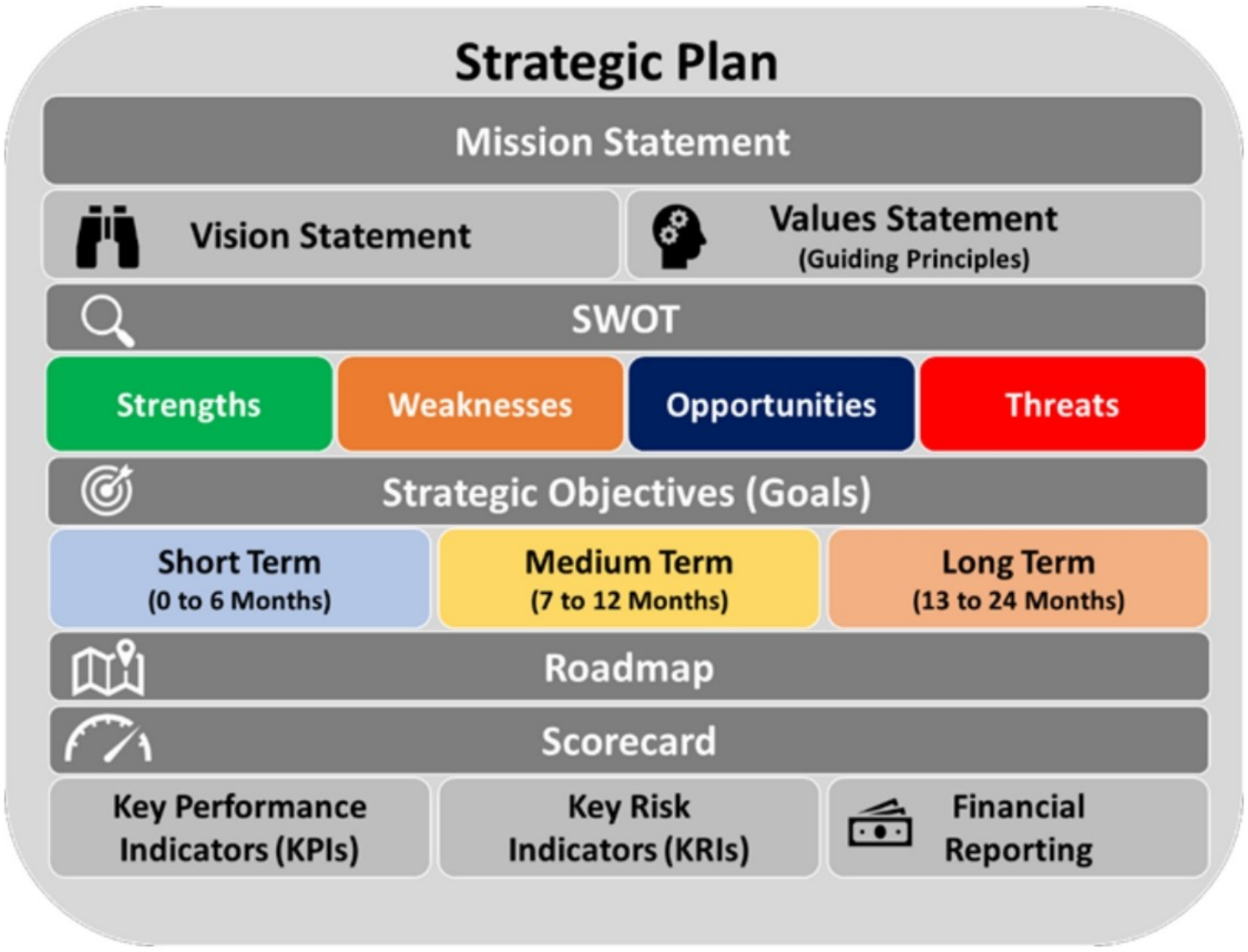


Figure 60: Strategic Information Security Plan Framework

Here is a discussion of each of the strategic plan components:

- **Mission Statement:** A mission statement is an overarching statement of the high-level aspirations or purpose of the information security program. It outlines what the CISO seeks to accomplish and declares why the information security program exists.
- **Vision Statement:** A vision statement summarizes the information security program's future direction, predicting what the program may look like in the future.
- **Values Statement:** A values statement contains the guiding principles and core values on which the organization's information security program will operate. Principles endure the test of time and form the foundation of the strategy.
- **SWOT:** A SWOT analysis identifies the strengths, weaknesses, opportunities, and threats of/to the information security program. This is where the CISO evaluates the program from the organization's viewpoint and its existing structure. For example, threats are to the security program, not threats to the organization.
- **Strategic Objectives:** Strategic objectives are the goals of the program over a specific time horizon, recommended to be at most three years for an information security program. Short-, medium-, and long-term goals typically segment the time horizon. The objectives identify what must be accomplished to achieve your vision for the information security program.
- **Roadmap:** A roadmap outlines the actions, timeline, and milestones necessary to accomplish the goals established for the information security program. Roadmaps vary in detail but are not meant to be project plans. They serve as a discussion document to communicate the program's strategic direction. A visual roadmap representation can be used to motivate, share, and aid team collaboration.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Scorecard:** A scorecard is a dashboard that reports the performance of the information security program. Typically, the dashboard is divided into Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), and the financial accounting of the IS program's budget. It tracks and reports on the program's performance against the monthly, quarterly, and annual targets.

KRIs are indicators to measure how risky an activity is and provide early warning of risk exposures. KPIs focus on the performance of the program's achievement of goals against the plan. Financial reporting provides reports on the program's spending against its planned budget.

The process of achieving goal-based planning comprises the following activities:

1.2.1. Strategic Planning Basics [111]

Strategic planning is an organizational management activity used to set priorities, focus energy and resources, strengthen operations, and ensure the organization works toward common goals. A strategic plan is a document communicating the organization's objectives, the actions needed to achieve those goals, and the other critical elements developed during the planning exercise.

Strategic Planning Steps

- **Assessment:** It helps understand the current internal and external environments.
- **Strategy formulation:** A high-level strategy is developed, and a basic organization-level strategic plan is documented.
- **Strategy execution:** The high-level plan is translated into more operational planning and action items.
- **Evaluation:** This involves the ongoing refinement and evaluation of performance, culture, communications, data reporting, and other strategic management issues.

1.2.2. Alignment to Organizational Strategy and Goals

One of the most critical responsibilities of a CISO is to align the information security program to an organization's strategy and goals. However, it is more than just the corporate strategy that the program must align with but also the Information Technology (IT) organization. In some organizations, the alignment must be extended to other parts of the business, including Enterprise Risk, Technology Audit, Information Privacy, Physical Protection, and Fraud Prevention. One of the primary functions of Enterprise Architecture within IT is alignment with the organization. However, a CISO should never assume this alignment is accurate but must verify to ensure the information security strategy aligns with IT and organizational priorities.

The following is an example of a Goals Alignment relationship model:

Figure 61: Goals Alignment Relationship Model

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.2.3. Defining Tactical Short, Medium, and Long-Term Information Security Goals

Information security goals are typically time-bound to ensure they are completed efficiently and effectively and are commensurate with the impact they could have on further protecting information and assets.

The following are examples of tactical time-bound goals:

Figure 62: Tactical Time-Bound Goal Overview

- **Short-Term Goals:** These goals should be developed with a finite amount of time and expense in mind. They should be the easiest to achieve as they consume minimal time and resources to accomplish the task. Short-term goals usually can be accomplished with little to no budget increase and can be approved by the CISO.
- **Medium-Term Goals:** These goals should result from an individual or team achieving or completing related tasks because of consistently satisfying the requirements of their short-term objectives. Medium-term goals may require increased Operating Expenses (OpEx), requiring additional funding. As a rule, these goals do not require a Capital Expense (CapEx).
- **Long-Term Goals:** These goals require budget allocation and planning for using internal and external resources. Long-term goals are more oversized cost items that may require a CapEx investment, senior management approval, and a Request for Proposal (RFP) issuance.

1.2.4. Information Security Strategy Communication

Developing a communication plan is one of the most critical planning activities within the information security program. The plan establishes the methods and processes that define how the program communicates internally and externally to broadcast its mission, vision, and values.

The following is a framework for developing a communications plan for an information security strategy:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 63: Information Security Strategy Communications Plan

- **Goals:** Establish clear, specific, measurable goals. The goals should be realistic because they leverage existing information security program resources.
- **KPIs:** Key Performance Indicators should be designed to gauge the effectiveness of the communication strategy. Particular attention should be paid to determining if the security culture is improving, if end user behavior is appropriate, and other vital indicators.
- **Schedule:** Communications should be regular and specific to build consistency and leverage message familiarity.
- **Media:** Several messaging media—banners, newsletters, email blasts, posters, surveys, and other methods of presenting the security message—should be used. Communication effectiveness can be enhanced by delivering messages to audiences in their preferred medium. To integrate the information security program message, consider how users receive information.
- **Message:** This is planned communications to manage various situations such as those below:
    - **Awareness:** A communications program includes awareness training and messaging to ensure users understand their roles and responsibilities in the information security program.
    - **Crisis:** A crisis communications plan should be in place to manage security breaches or other operational disruptions.
    - **Training:** Specific types of training can be designed to promote a culture of security, ranging from secure application coding to sensitive data handling.
    - **Testing:** One of the more effective ways to message security importance is to evaluate. Recognizing phishing attacks and avoiding social engineering attacks are high-value testing strategies.
- **Audience:** Know your audience, whether internal or external. Communication approaches will differ by audience; the right approach can help the messaging strategy.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Communications must be tailored for executives, media, law enforcement, or other specialized audiences.

1.2.5. Creating a Culture of Security

CISOs need to change the culture within the organization to a state of security-aware employees to avoid an uphill battle in protecting information and assets. What is culture, and how can a CISO change it? Sociologists have defined culture as a group's collective customs, beliefs, and general attitude. Organizations typically have one of two types of security culture: apathetic or security aware. An information security program is the foundation of an organization's security culture, and a CISO must invest resources in cultivating a security-aware culture.

Improving the security culture will only be possible if the information security program is viewed positively. Organizations that view the program simply as an overhead or an obstacle to business must change their perception before accurate alignment can occur. Changing these perceptions will require some understanding of organizational behavior.

The CISO must work to shift negative perceptions about information security to positive ones to build a culture of security. The CISO must demonstrate that the information security program provides significant value by managing or mitigating risks that could interrupt critical business functions.

Influencing the Culture of Your Organization [110]:

The following are four primary ways to influence the culture of an organization:

- **Emphasize what is Important:** Communicate the goals of the information security program and how they are aligned with the business. Be bold in talking about accomplishments and emphasize the behaviors desired by end users.
- **Reward Employees:** Users who demonstrate responsible computing and reporting security issues should be rewarded to reinforce the security-aware culture.
- **Discourage Behaviors:** Security should not be punitive but discourage bad security behavior. A CISO should dissuade users from continuing unwanted behaviors by giving them constructive feedback. If the behavior continues, it may be necessary to issue verbal warnings, written warnings, or termination of employment.
- **Model Desired Behavior:** One of the most potent ways to influence behavior in the workplace is to model acceptable behavior. For example, share how one department's security incidents are lower than all others.

Once the CISO begins to influence the organizational culture, the work required to establish an information security culture throughout the organization starts. Corporate culture reflects the personality of the top leadership of an organization. Similarly, information security culture in an organization often reflects the character and nature of the CISO.

Information security culture established at leadership levels of the organization increases opportunities to align with the culture of the organization. This enables aligning security programs and services to the needs of the organization.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. DESIGNING, DEVELOPING, AND MAINTAINING AN ENTERPRISE INFORMATION SECURITY PROGRAM

Before construction begins on a new home, homeowners and contractors must agree on what the house will look like, the number of rooms, and their sizes. Building a cybersecurity program should be no different. You may be surprised at the number of cybersecurity programs built, costing significantly more than an average home, that need a basic blueprint. Many organizations align to either ISO 27001 or NIST SP 800-53. However, this does not necessarily serve as a blueprint.

A blueprint is a guide for making something and consists of drawings, pictures, and instructions. It aims to communicate the end result to everyone involved in constructing that something. In a cybersecurity program, an architect uses a blueprint to share the program's vision without committing to specific implementation details. For example, an architect may identify the need for a Cyber Security Operations Center (CSOC) but leave the specifications of the CSOC open for stakeholders to decide. Stakeholders may build a CSOC or contract for CSOC services from a Managed Security Services Provider (MSSP).

A blueprint serves as the comprehensive plan identifying the structure and components of your information security program. It provides a model of the finished product. Euler diagrams are perfect for creating cybersecurity program blueprints. A Euler diagram is a method used to represent sets and their relationships, often overlapping shapes to suggest scale and relationship.

The following is an example of a cybersecurity program blueprint:

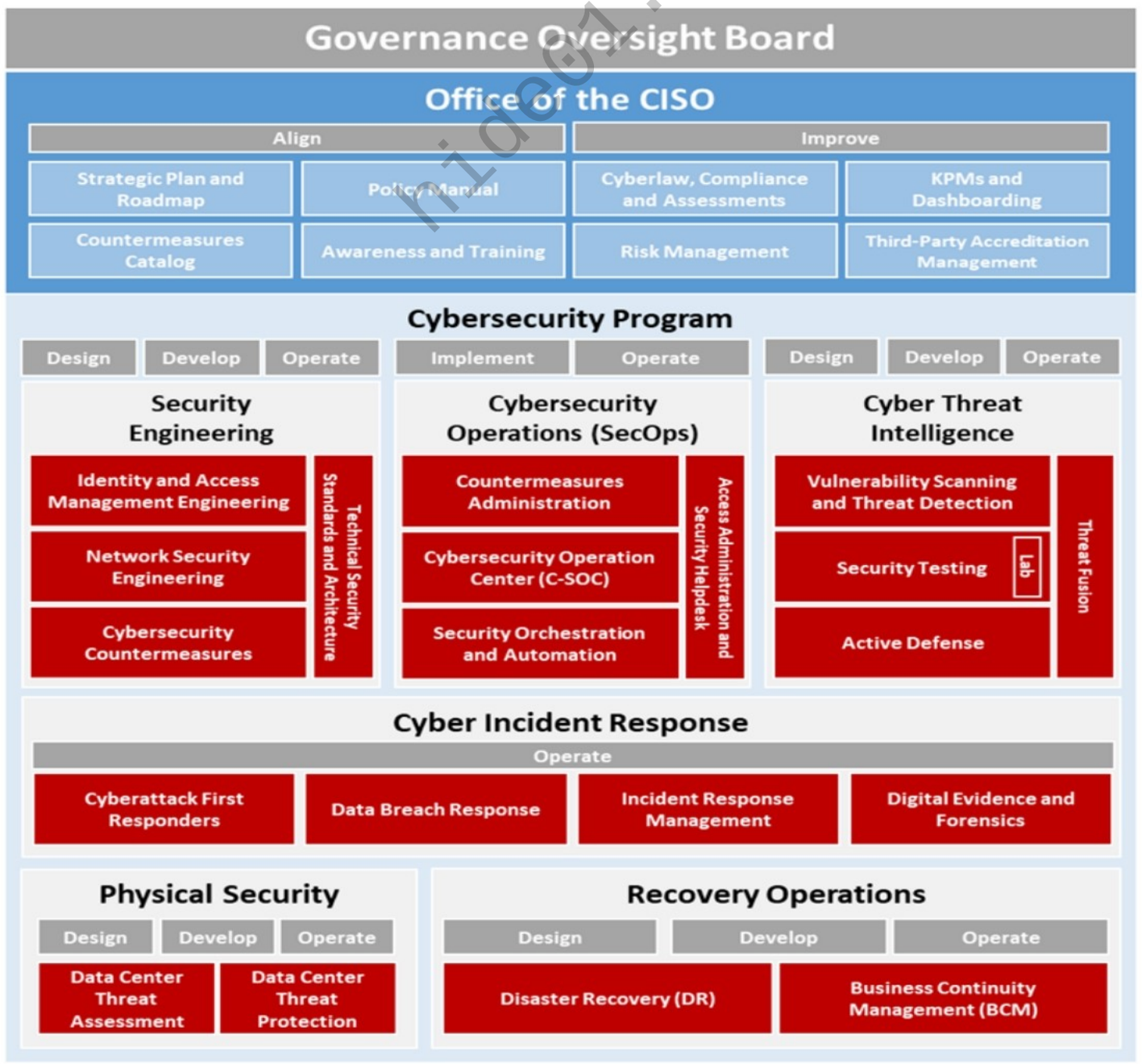


Figure 64: Cybersecurity Program Blueprint. (By Tari Schreider, licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 International License)

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2.1. Ensuring a Sound Program Foundation

A well-structured information security program should have a sound architecture as its foundation. Unfortunately, the word *architecture* has come to mean so many things in the information security world that it is easy to misunderstand the concept. CISOs should think of *architecture* in the context of design. For example, when someone says the name Frank Lloyd Wright, the iconic nature of his architecture immediately comes to mind. Observers can anticipate a consistent experience when encountering any of his designs. Similarly, CISOs should choose to present the creation of their information security program to their management and peers in a way that will be accessible and expected in their corporate context. CISOs should begin their design journey believing they are architects, and their tradecraft is architecture. They should use blueprints, frameworks, and models to build an architecture. CISOs need to think like an architect to be an architect.

The following simple figure shows one view of an information security architecture as a schema:

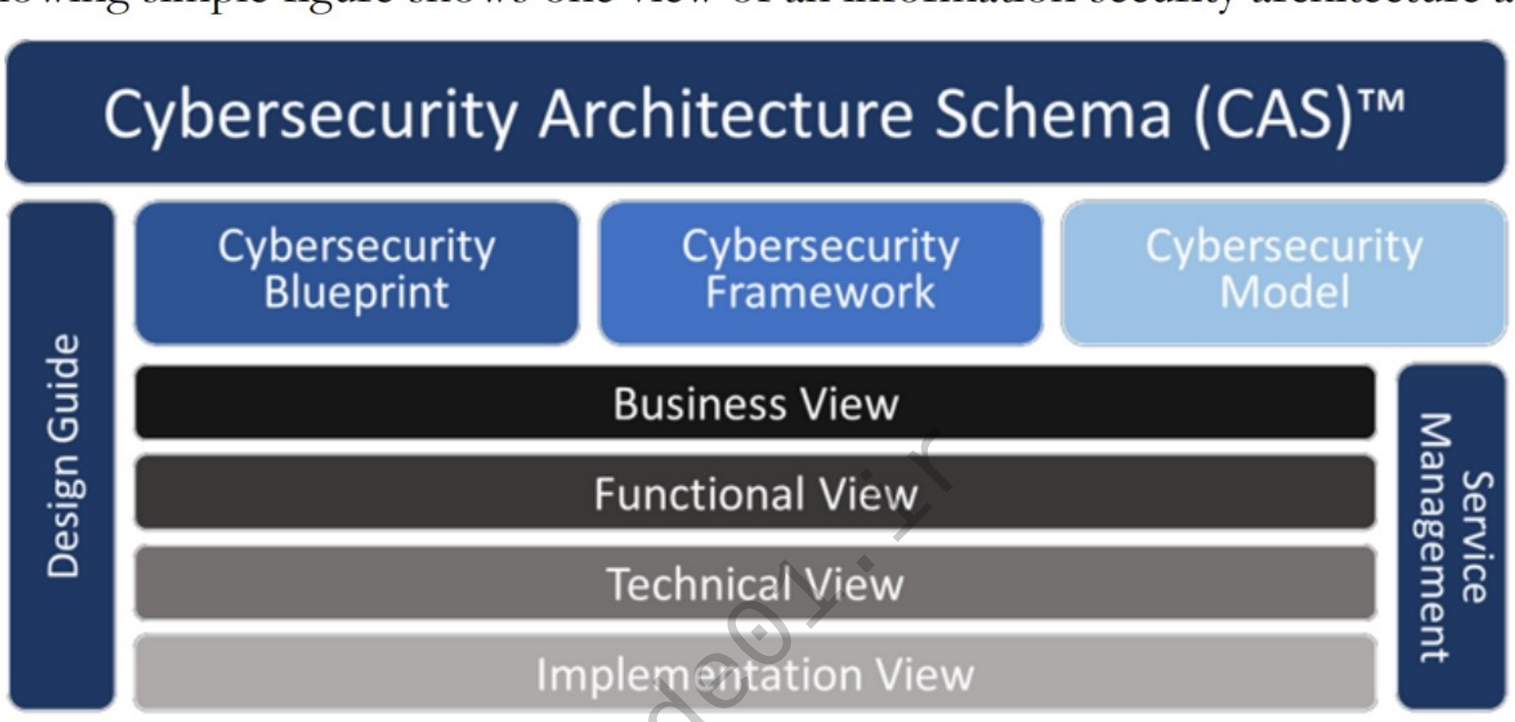


Figure 65: Cybersecurity Architecture Schema (CAS)™. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License)

2.2. Architectural Views

It is often challenging to show someone an entire blueprint or architecture and hope it all sinks in. Designs need to be more complex to be fully understood by stakeholders in a single presentation. One reason is that only some people will be interested in the entire architecture while others only want to see what applies directly to them. To accommodate this, the architecture community uses views or layers of the whole design to represent areas of the design specific to certain stakeholders. The combination of the views constitutes the entire design. When building a house, there would be separate architectural views for the frame, plumbing, electrical, etc. Views have been a mainstay of IT architecture for over 30 years. Refer to the ISO/IEC/IEEE 42010 website at www.iso-architecture.org/ieee-1471/index.html to learn more about architectural views and IT architecture. Four views are used in information security program designs for their relevance, simplicity, and effectiveness. These views are business, functional, technical, and implementation.

- **Business View—the Why:** The business view answers, "Why are we doing this?" This view addresses the requirements and concerns of the users from their business perspective. Here, define what the cybersecurity program is intended to accomplish, what basic functionality it should have, and the type of usability envisioned. This is where the cybersecurity program is aligned with key business drivers. For example, the business may

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

want more speed and agility, which can be accomplished by empowering customers to perform some security functions themselves.

- **Functional View—the What:** The functional view answers, "What should it do?" This view is concerned with the required capabilities of the cybersecurity program. For example, speed and agility would require the program to provide self-service capabilities for customer password resets. In this view, we are not concerned with how that would be performed, just that the program should provide that functionality.
- **Technical View—the How:** The technical view answers, "How should it be done?" This view establishes the preferred approach to provide critical capabilities. From the functional perspective, we stated that password self-service would provide the improved speed and agility that the business requires for customers. The business would use a Single Sign-on (SSO) solution or an Identity and Access Management (IAM) provisioning system supporting password resets. This view is not concerned with the specific product that would be used.
- **Implementation View—with What:** The implementation view answers, "What will we use?" This view concerns the details of the products and solutions required to implement the technical view. Following our previous example, we would select a product that provides SSO and IAM to allow password resets. The technology is the last layer of the design to ensure you do not acquire products before all the requirements are met in the design.

2.3. Creating Measurements and Metrics

hideo1.ir

Evaluation is a necessary component of strategic planning. This phase ensures activities occur to measure the effectiveness of planning and performance during execution so the organization can improve performance. The most common evaluation tool for strategic planning is the Key Performance Indicator (KPI).

KPIs are performance measures that indicate progress toward a desirable outcome. In strategic planning, KPIs monitor the implementation and effectiveness of an organization's strategies by highlighting gaps between actual and targeted performance. KPIs are a metric used to evaluate critical success factors.

KPIs defined for the security program must reflect the organization's goals and objectives. The organization should develop a unique set of KPIs to determine the expected outcome in each project or service. For example, the Chief Information Officer (CIO) will have outcomes defined for IT service delivery, the Chief Financial Officer (CFO) will have outcomes defined for enterprise financial management, and sales will have outcomes defined in terms of quotas and revenue generation. Each of these programs provides input into the KPIs developed for security.

Like any evaluation in the security program, the quality of the measurements is essential. The KPIs that measure the performance of the information security strategy must yield quantifiable information. The data must also be readily obtainable, and the data collection process to support the evaluation should be repeatable.

Finally, the KPI measurements must help track performance and direct resources. KPIs must be quantifiable because performance measurements cannot be subjective if the organization intends to determine whether performance gaps exist, which would require adjustments in the strategy.

Beyond the typical characteristics of good metrics, KPIs must be verifiable and ensure data

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

collection accuracy. Good KPIs should provide the following:

- Objective methods to see if the strategy is working
- Comparison to gauge performance change over time
- Tools to focus attention on what matters most to success
- Measurement of accomplishments, not just of the work that is performed
- Common language for communication
- Tools to reduce intangible uncertainty
- Measurement of the right things

2.4. Balanced Scorecard

The balanced scorecard is a strategic planning and management system used to align business activities with the vision and strategy of the organization, improve internal and external communications, and monitor the organization's performance against strategic goals.

The Balanced Scorecard Perspectives **[112]**

The balanced scorecard suggests that CISOs view the organization from four perspectives and develop metrics, collect data, and analyze it relative to each of these perspectives:

- **The Learning and Growth Perspective** includes employee training and corporate cultural attitudes related to individual and corporate improvement. Metrics can be implemented to guide managers in focusing training funds where they can help the most.
- **The Business Process Perspective:** It refers to internal business processes. Metrics based on this perspective allow the managers to know how well their business is running and whether its products and services conform to customer requirements (the mission).
- **The Customer Perspective**: It focuses on customer satisfaction in the business. Surveying customers determines the customer perspective to assess their level of satisfaction with the cybersecurity program. It is critical to manage customer satisfaction and program perception. If customers are unsatisfied, they will eventually find other suppliers to meet their needs.
- **The Financial Perspective:** The value of the IS program can be demonstrated through investment transparency, where program investments are linked to specific activities that reduce risk, the monthly burn rate of the budget, and the cost per employee to manage risk. Showing the annual cost of the IS program as a percentage of the overall IT budget is widely recognized as a critical indicator.

2.5. Continuous Monitoring and Reporting Outcomes

NIST Special Publication 800-137 [113]— Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. The purpose of this guideline is to assist organizations in developing a continuous monitoring strategy and implementing a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance and the information needed to respond to risk promptly should observations indicate that the security

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

controls are inadequate.

Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The following section describes the process for developing an ISCM strategy and implementing an ISCM program, including activities at the organization, mission/business process, and information systems tiers. A well-designed ISCM strategy encompasses security control assessment, security status monitoring, and security status reporting in support of timely risk-based decision-making throughout the organization. It also incorporates processes to ensure that response actions are taken. An organization's strategy for action based on data collected is as important (if not more critical) as collecting the data. The ISCM strategy for defining an ISCM program is as follows:

Figure 66: Information Security Continuous Monitoring (ISCM) Strategy

- Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting—automate collection, analysis, and reporting of data where possible.
- Analyze the data collected and report findings, determining the appropriate response. Collecting additional information to clarify or supplement existing monitoring data may be necessary.
- Respond to findings with technical, management, and operational mitigating activities or risk acceptance, transference/sharing, or avoidance/rejection.
- Review and update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities. Further enable data-driven control of the security of an organization's information infrastructure and improve organizational resilience.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2.6. Continuous Improvement

A continual improvement process, often called a Continuous Improvement Process (CIP), is an ongoing effort to improve products, services, or processes. These efforts can result in *incremental* improvement over time or *breakthrough* improvement all at once. Delivery processes are constantly evaluated and improved in efficiency, effectiveness, and flexibility. Some see CIPs as a meta-process for most management systems. W. Edwards Deming, a pioneer of the field, saw it as part of the delivery process and the design of the delivery process itself.

2.7. Information Technology Infrastructure Library (ITIL) Continual Service Improvement (CSI)

CSI continually improves the effectiveness and efficiency of services and processes. As per ITIL 2011, the following main processes are part of the ITIL Continual Service Improvement (CSI) stage:

- *Service Measurement* is a defined process in the CSI volume of ITIL v3. Service measurement indicates that organizations now think beyond the physical infrastructure when delivering IT services.
- *Service Reporting* reports on operationally and strategically achieved results. It also says any developments related to Service Level Agreements (SLAs), such as hitting various targets, like availability.
- *Service Improvement* defines specific initiatives to improve cybersecurity services and processes based on the results of service reviews and process evaluations. The resulting initiatives are either internal initiatives pursued by the service provider on his behalf or initiatives requiring customer cooperation.

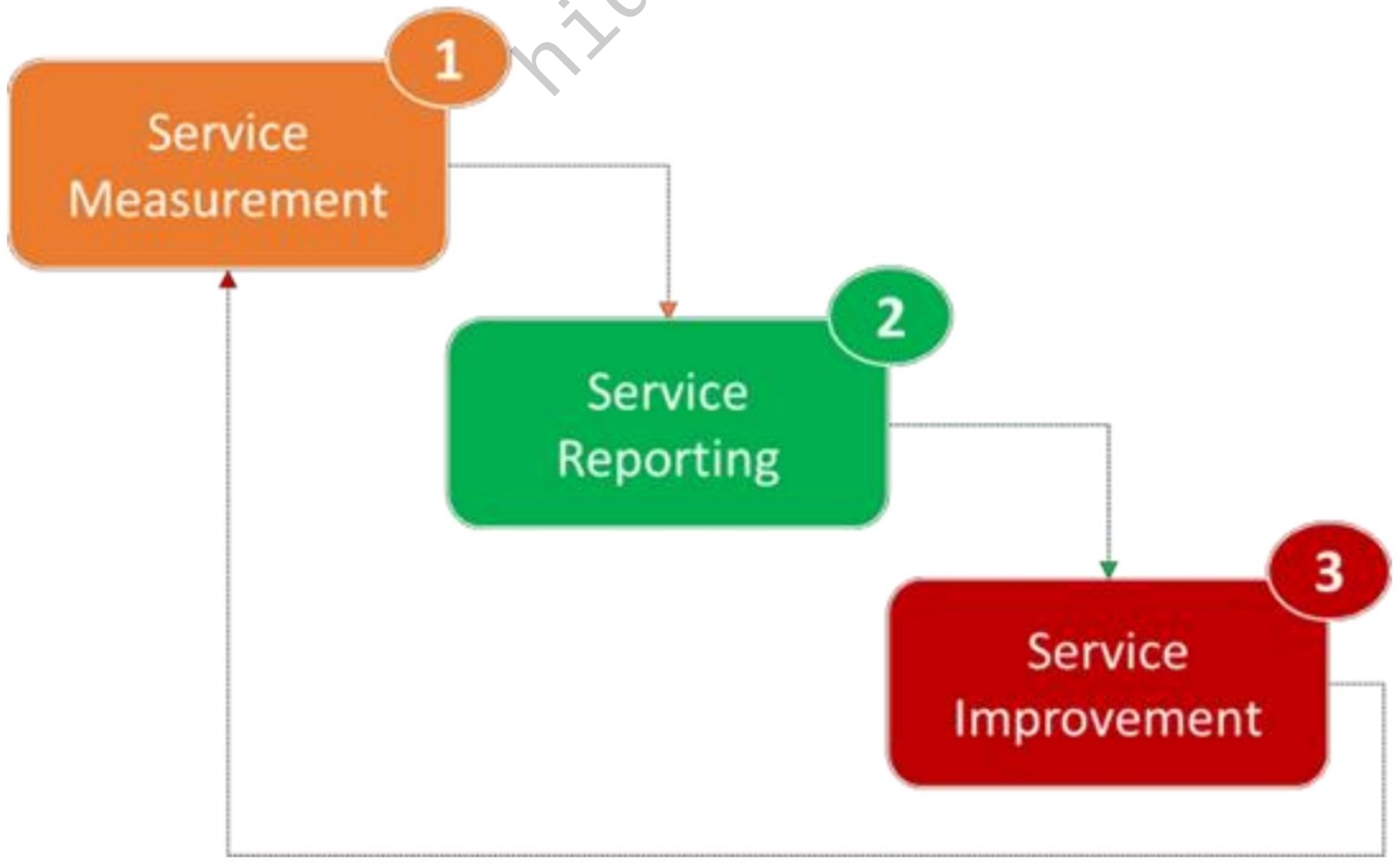


Figure 67: Information Technology Infrastructure Library (ITIL) Continuous Improvement Process (CIP) Model

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. UNDERSTANDING THE ENTERPRISE ARCHITECTURE (EA)

CISOs must understand the technical domain being monitored, and this begins with understanding the organization's Enterprise Architecture (EA). An EA is both a result and a process. From a process perspective, it is a well-defined practice for performing analysis, design, planning, and technology implementation. The result is the outcome of the EA process.

Security operations depend on data provided by the EA program to identify the organization's business processes and technology infrastructure. Complex technical environments may require multiple security operations teams so that the program can assign specific processes and procedures to unique environments.

EA supports planning and decision-making through documentation and information that provides an abstract view of an enterprise at various levels of scope and detail [114]. EA provides a framework to define business requirements, rules, and cases that will lead the organization to accomplish its mission, vision, and purpose. The purpose of EA is to optimize across the enterprise the often-fragmented legacy of processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the delivery of the business strategy [114]. This is valuable for all organizations but is critical in large, complex environments.

Once established and documented formally, these business-related concerns provide the foundation upon which an organization builds the technology, communications, and security infrastructure that will support all business processes. The rules, standards, and tools used to create an EA are business-centric; however, this discipline requires support from IT and security leaders, including the CIO and CISO, to achieve its goals. The effort to produce an accurate and comprehensive EA will bring together business and technology leaders, which is beneficial for increasing the opportunity to align business, IT, and security within an organization.

An organization's EA should be an integrated project team component to ensure the sub-architectures integrate with the EA and are planned, mapped, and executed correctly. Then, EA can exist as an abstract layer that provides structure and enhances an organization's technology infrastructure, network architecture, and security architecture. Once established, the EA allows harmonious coordination with IT and information security—the technological components of EA function as an enabler to support business processes. However, business processes need clear and formal definitions to select the best technology to enhance and support it.

Effective implementation of EA allows the seamless integration of protection measures into business rules and processes. For example, technology and security leaders can better understand the information provided by detective controls deployed in the enterprise by mapping them into the EA and defining a security model that considers the interactions of business processes and data flows at a granular level. The enhanced visibility provided by this approach offers context related to anomalies and violations of business or security rules. It improves the ability of the organization to prioritize response efforts according to business impact. A mature and comprehensive implementation of EA could allow an organization to adopt potentially controversial solutions like the consumerization of IT, the Internet of Things (IoT), and Bring Your Own Device (BYOD).

Linking EA with the business or security architecture is only realistic in a mature organization. However, this effort provides significant value from a governance perspective: it forces collaboration, buy-in, and understanding throughout the organization as it relates to the needs of the business and

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the interaction between business processes and other aspects of the enterprise environment.

Linking the IS program to EA is a crucial aspect of advancing IS program activities through the maturity levels of the Capability Maturity Model Integration (CMMI) model.

3.1. EA Types

Various approaches for developing EA exist. Some options are more flexible than others, and each option applies differently depending on the type and objectives of the organization. The framework an organization selects is critical because EA, among other considerations, influences change management, infrastructure management, security controls, and application development.

3.1.1. The Zachman Framework:

The Zachman Framework is "considered an ontology or schema to help organize enterprise architecture artifacts such as documents, specifications and models" [115]. Many versions of EA have roots in the effort completed by Zachman to develop the *Zachman Framework*.

The Zachman Framework answers the questions of what, how, where, who, when, and why, as they relate to critical attributes of the enterprise. An organization can formalize a definition of the EA to support governance activities associated with this detailed enterprise classification.

The Zachman Framework for Enterprise Architecture [116] is typically depicted as a bounded 6 x 6 matrix with the Communication Interrogatives as Columns and the Reification Transformations as Rows. The framework classifications are represented by Cells, which are the intersection between Interrogatives and the Transformations. This matrix constitutes the total set of relevant descriptive representations for describing anything: an enterprise, for instance.

The following is an image of the Zachman Framework:

hi_de01_if

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

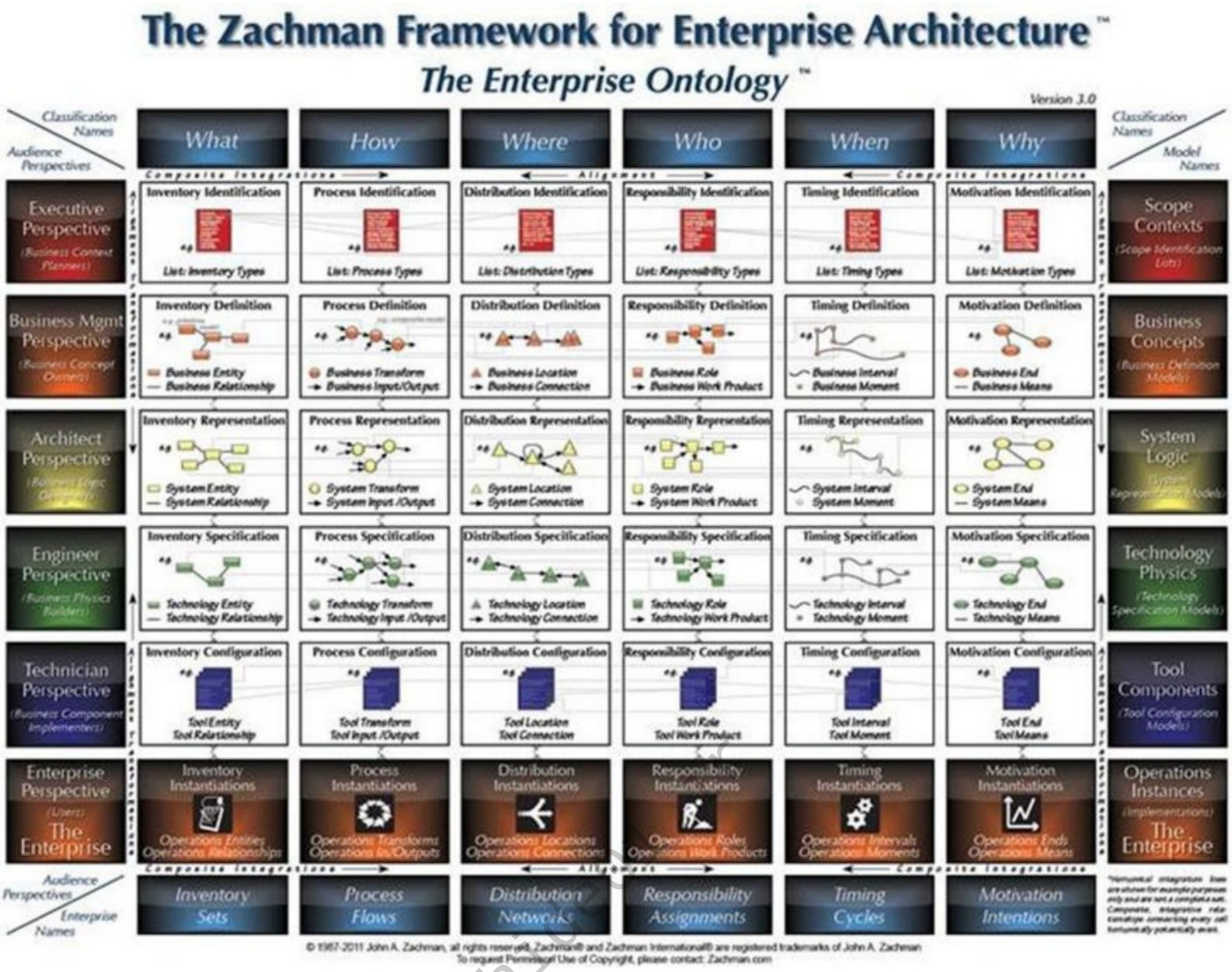


Figure 68: Zachman 6 x 6 Matrix

Due to its complexity and level of detail, the Zachman Framework is a tool best suited for large enterprise environments. Smaller organizations with adequate resources can use some portions of the matrix to define a comprehensive EA. Other architecture frameworks exist to support this effort in smaller or less complex enterprises.

3.1.2. The Open Group Architecture Framework (TOGAF)

TOGAF is a business-centric EA framework that provides flexibility for formally defining business activities. TOGAF provides a structured approach for organizations seeking to organize and manage technology implementation in the enterprise. However, organizations and activities within groups can focus on specific subsets of the framework to accomplish their goals. The flexibility of TOGAF makes this framework effective for activities that range from small development projects to comprehensive Enterprise Resource Planning (ERP) systems.

The Open Group Architecture Framework [117]

The structure of the TOGAF documentation reflects the design and content of an Architecture Capability within an enterprise. The TOGAF specification exists as seven independent parts that allow different areas of specialization to be considered in detail and addressed in isolation. Although all components work together, selecting elements for

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

adoption while excluding others is also feasible.

- **PART I** (Introduction): This part briefly introduces the critical concepts of EA and the TOGAF approach. It contains the definitions of terms used throughout TOGAF and release notes detailing the changes between this version and the previous version of TOGAF.
- **PART II** (Architecture Development Method): This part is the core of TOGAF. It describes the TOGAF Architecture Development Method (ADM)—a step-by-step approach to developing an EA.
- **PART III** (ADM Guidelines and Techniques): This part contains a collection of guidelines and techniques for applying TOGAF and the TOGAF ADM.
- **PART IV** (Architecture Content Framework): This part describes the TOGAF content framework, including a structured meta-model for architectural artifacts, reusable architecture building blocks, and an overview of typical architecture deliverables.
- **PART V** (Enterprise Continuum and Tools): This part discusses taxonomies and tools to categorize and store the outputs of architecture activity within an enterprise.
- **PART VI** (TOGAF Reference Models): This part provides a selection of architectural reference models, including the TOGAF Foundation Architecture and the Integrated Information Infrastructure Reference Model (III-RM).
- **PART VII** (Architecture Capability Framework): This part discusses the organization, processes, skills, roles, and responsibilities required to establish and operate an architecture function within an enterprise.

The following is a graph of The Open Group Architecture Framework (TOGAF) Architecture:

hi_dee1_ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

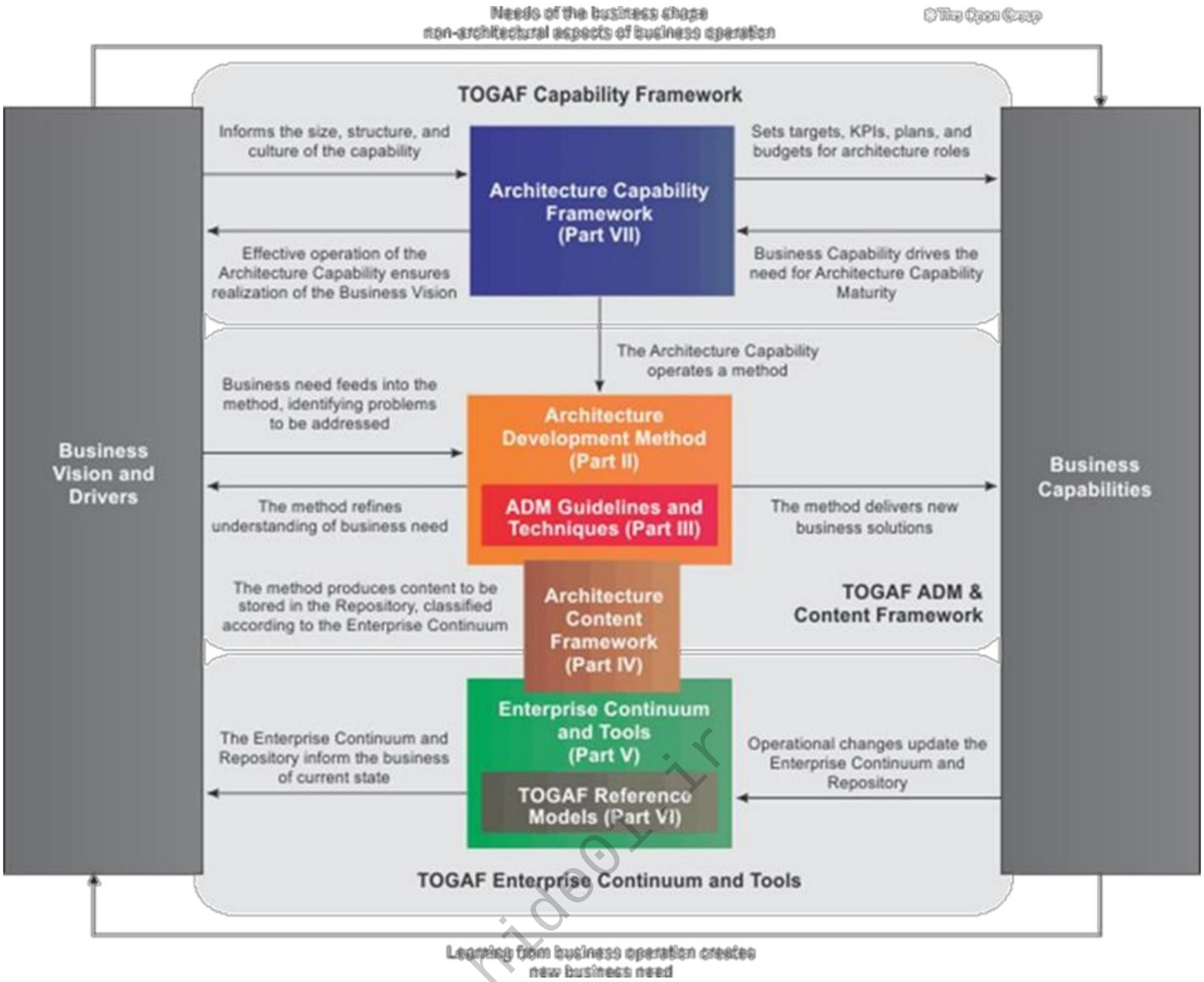


Figure 69: Structure of The Open Group Architecture Framework (TOGAF) Architecture

Any organization considering or in the business transformation process will benefit from using TOGAF. In particular, "organizations that seek to implement Boundaryless Information Flow (BIF) can use TOGAF to define and implement the structures and processes to enable access to integrated information within and between enterprises" [117]. An infrastructure providing BIF has open standard components that deliver services in a customer's extended enterprise that combine multiple sources of information and securely deliver the data whenever and wherever it is needed, in the proper context for the people or systems using that information [117].

3.1.3. Sherwood Applied Business Security Architecture (SABSA)

The Sherwood Applied Business Security Architecture (SABSA) is a framework and methodology used to meet various enterprise needs: risk management, information assurance, governance, and continuity management. SABSA is valuable because the framework ensures that security services are designed, delivered, and supported as an integral part of your business and IT management infrastructure. The goal is that the security architecture is fully integrated into the EA [72].

The SABSA Process [72]

SABSA comprises a series of integrated frameworks, models, methods, and processes used

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

independently or as a holistic, integrated enterprise solution, including:

- Business Requirements Engineering Framework (known as Attributes Profiling)
- Risk and Opportunity Management Framework
- Policy Architecture Framework
- Security Services–Oriented Architecture Framework
- Governance Framework
- Security Domain Framework
- Through-life Security Service Management and Performance Management Framework

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

hidedt.ir

Table 27: SABSA 6 x 6 Matrix

SABSA produces a 6 x 6 matrix called the SABSA Master Matrix, like the Zachman Framework. Beyond their matrices' similarities, SABSA differs from Zachman's Framework because of the focus on integrating security in the EA.

3.1.4. Federal Enterprise Architecture Framework (FEAF)

The Federal Enterprise Architecture Framework (FEAF) is a set of tools that help US federal agencies define the structure of EA within each organization. It allows the agencies to describe the current enterprise in appropriate detail and identify how it should look in the future so each organization can plan to transition from the current state to the future state. The FEAF also provides a mechanism for agencies to map the architecture to the strategic plan defined by each organization.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Federal Enterprise Architecture Framework (FEAF) v2 [114] FEAF v2 describes a suite of tools to help government planners implement the Common Approach. At its core is the Consolidated Reference Model (CRM), which equips the U.S. Office of Management and Budget and federal agencies with a common language and framework to describe and analyze investments. It consists of a set of interrelated *reference models* that describe the six sub-architecture domains in the framework:

- Strategy
- Business
- Data
- Applications
- Infrastructure
- Security

These are designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across agencies. Also, by applying all six reference models, agencies can establish a line of sight from the strategic goals at the highest organizational level to the software and hardware infrastructure that achieves those goals. The reference models comprise a framework for describing essential elements of federal agency operations familiarly and consistently.

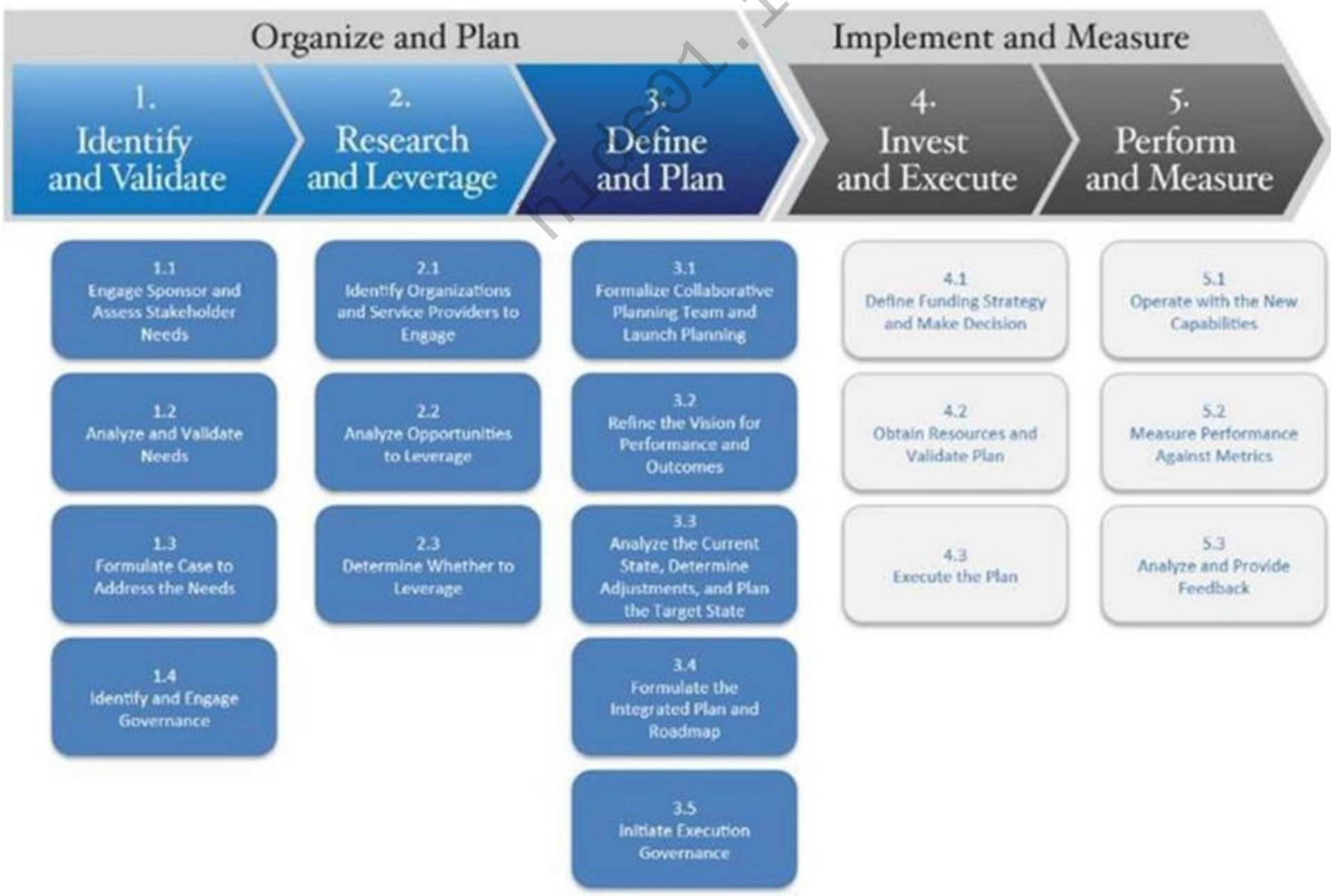


Figure 70: Federal Enterprise Architecture Framework (FEAF)

FEAF v2 was developed for agencies of the U.S. Federal Government; however, the models provided by this EA framework support various nongovernmental organizations.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations that conduct business with the U.S. Federal Government benefit from defining a comprehensive EA using FEAF because federal partners easily understand it, and the framework provides a structure for connecting the organizations to exchange information.

4. FINANCE

Financial management defines the processes of planning, organizing, directing, controlling, and reporting the monetary activities of an organization and the use of its funds.

The CISO plays a significant role in financial planning for the information security program. Considering most of the funding for the security program is allocated from the organizational operating budget, the CISO has a fiduciary responsibility to ensure prudent utilization of the funds allocated to the program. Good stewardship requires a solid grasp of fundamental financial management concepts. This understanding promotes the economic success of the security program and its mission.

4.1. Understanding Security Program Funding

Organizations spend an average of 5.6 percent of the overall IT budget on IT security and risk management, according to the most recent IT Key Metrics Data from Gartner, Inc. [118]. One of the top challenges for a CISO is identifying funding sources for an information security program.

Most budget requests are accompanied by an ROI (Return On Investment) analysis. This is the language your financial team understands and is most comfortable with. A positive ROI is usually the difference between a positive and an adverse decision on funding. However, cybersecurity budget requests are more difficult to quantify. Security ROI is typically expressed by comparing security investments with the potential liabilities arising from security breaches. This is like calculating the financial benefit of insurance for physical assets, such as buildings and equipment.

ITdet.ir

However, simply providing a well-defined ROI only sometimes guarantees success. When approaching senior management and your financial team when seeking funding, there are several additional considerations.

Initiating the budget discussion requires emphasizing cost avoidance over profits, supported by concrete, empirical evidence illustrating business risks and associated costs. Interestingly, the specific nature of the threat, while critical to the security team, means less with the financial staff. Their primary concern is the economic impact on the organization. Therefore, the best way to approach senior management to fund your cybersecurity program is to explain the expenditures using an ROI approach.

4.2. Analyzing, Forecasting, and Developing a Security Budget

Budgeting is an essential financial management process to estimate revenue and expenses over a specified period. Counting and matching costs to revenue (actual or anticipated) helps determine whether enough money exists to fund operations or expand programs.

Budgets are invaluable because they demonstrate the trade-off made when one resource is exchanged for another. For the CISO, the security budget measures the exchange of financial allocations for the security products and services supporting the organization. For a successful continuation of this exchange throughout the lifespan of the security program, the CISO must manage the budget effectively. This will help determine whether the budget is in surplus, balanced,

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

or deficit, which will assist in determining adjustments. Ideally, the budget managed by the CISO should either augment revenue, curtail costs, or mitigate risks.

CISOs requiring assistance with planning and managing program budgets can use the following checklist as a starting point to build a successful financial management program:

- Understand organizational financial standards.
- Document and track the budget.
- Account for slack.
- Manage costs.
- Periodically audit and evaluate budgets.
- Carefully select vendor services and supplies.

CISOs rarely have a background in accounting, but most organizations have a CFO or other financial leader who can provide insight into organizational financial management standards. Suppose no corporate standards for financial management exist. In that case, the CISO can obtain guidance from the Financial Accounting Standards Board (FASB), which publishes rules that define how corporations must account for their business activities.

The budget should account for slack, which represents an underestimation of revenue or an overestimation of expenses. The budget should provide adjustments for excesses or shortfalls because of planning estimates. Managing costs is a function of how the information security program operates. Finding the best value offered by services and suppliers is a good strategy. Just as controls are audited for effectiveness, the CISO should also audit the budget for accuracy and effectiveness. Once created, budget estimates must be revised and adjusted periodically or as new information becomes available about trends in spending history, changes in resource requirements, or organizational priorities.

hiredi.ir

The following checklist will help CISOs with securing proper funding:

- **Build a Relationship with the CFO:** CISOs are known for asking for money to fund initiatives that others might not perceive to add value to the business. One way to curb this opinion is to build a relationship with the CFO before asking for funding.
- **Understand Organizational Finance Strategies:** If a CISO does not understand their organization's finance strategy, it puts them at a disadvantage. For example, CISOs risk a denial of their funding request if they ask for CapEx funding when they should be asking for OpEx.
- **Avoid the FUD Factor:** Using fear, uncertainty, and doubt, or, in other words, scare tactics, can quickly backfire on a CISO if the negative outlook is not real. CISOs should use sound business logic to present their funding cases.
- **Demonstrate Competence:** To be perceived as a competent manager of department finances, CISOs must demonstrate command over finance fundamentals.
- **Demonstrate Business Value for Investment:** Although it may be difficult to show ROI for security investments, CISOs can demonstrate value for their investment funding request. Value can come in a variety of ways, including reduced risk and lower cost of operations.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Become a Wise Steward of Funding:** A CISO must prove that every dollar invested in the information security program has been spent wisely. Purchasing security technology and then letting it sit for months or replacing a recently acquired product before completing the lifecycle of it may not be viewed favorably by the organization's CFO.

4.2.1. Resource Requirements

Resource estimation is a structured prediction of the cost and other resources required to accomplish a task. One of the primary functions of the process is to establish a control basis. Therefore, the more accurate the estimation, the more dependable the control system becomes.

The required accuracy and effort going into resource estimation can be influenced by the uncertainty and risk involved because of the technical complexity and novelty of the project. The expected price basis of the contract could make resource estimation a critical factor. The higher the risk, the more important it becomes to have a realistic estimation, which implies a more detailed process.

The effort it will take to complete a task is also essential. Effort is determined by the time it will take to complete a task. Once the step required for the project is understood, resources can be assigned to determine how long the project will take and estimate human resources and other resource costs.

An adequately documented resource plan will specify the exact quantities of human resources, equipment, and materials required to complete the project.

Given the frequency and scale of security breaches and cyberattacks, it is no surprise to find *Information security/privacy* leading the Computer Economics' Net Percentage of Organizations Increasing Spending by Budget Category across all sectors [119]:

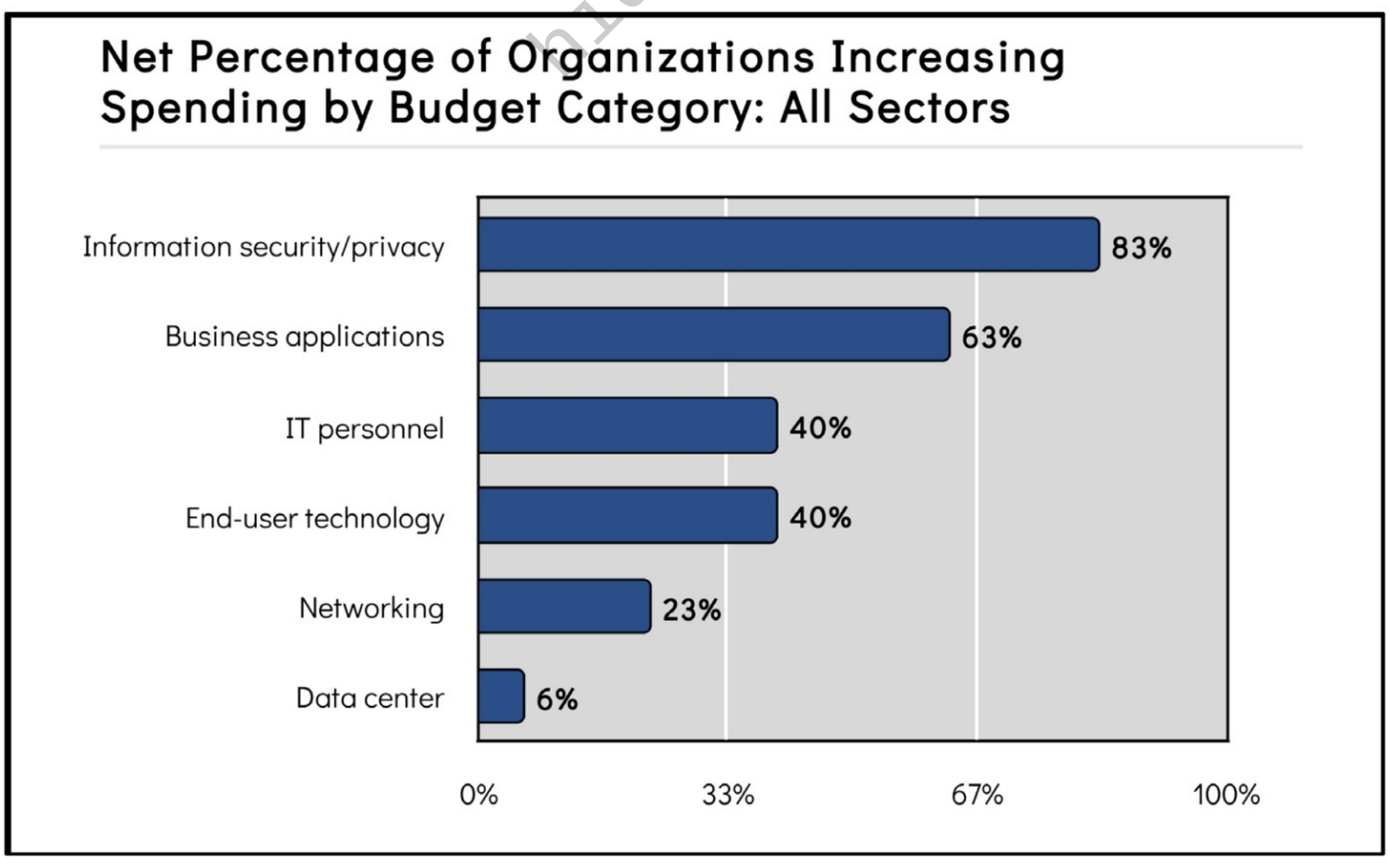


Figure 71: IT Spending and Staffing Benchmarks study for 2022/2023

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4.2.2. Define Financial Metrics

Each financial metric conveys a unique message about a body of economic data. In that way, financial metrics are like descriptive statistics. For instance, the statistical average (arithmetic mean) reveals the typical value in a data set.

Similarly, each financial metric reveals specific characteristics of the economic data set. Usually, those characteristics need to be clarified when merely reviewing the data. Cash flow investment metrics, for instance, measure investment performance by evaluating the series of cash inflows and outflows that follow from the investment. One of these metrics, the payback period, measures the time required for returns to cover costs. Potential investors can compare payback periods of different investments to help decide which is the better investment. The break-even point is the volume that must be sold at equal total cost and total revenue. The project is profitable if it can increase sales volume to the break-even point.

Prudent investors will also analyze the same investment choices with other metrics besides the payback period. Investors can use Net Present Value (NPV), Return on Investment (ROI), and Internal Rate of Return (IRR) to analyze the same investment choices.

4.2.3. Technology Refresh

A technology refresh cycle establishes a predictable process for swapping old technology with new assets every few years. Many benefits come with an established technological refresh cycle that makes the process worthwhile. Proactively managing technology to avoid production failures is an essential continuity of an operational strategy. Continuing to run outdated technology risks making the attack surface susceptible to vulnerabilities that can no longer be patched or mitigated.

CISOs should review their IS program technology in the following three ways:

Technology Obsolescence: CISOs should ensure they rely on something other than security technology that has passed its useful life. This can result in expensive maintenance, a lack of trained resources to support the technology, and the technology's inability to address current threats.

Technology Innovation: CISOs should continually surveil the cybersecurity technology landscape for innovative and effective ways of reducing risk and improving their program. However, caution is encouraged when selecting emerging technologies to avoid selecting solutions that cannot demonstrate actual value for threat and vulnerability mitigation and management.

Decrease Failure Rate: Using technology that has stayed within its meantime-to-failure rating is an approach for increasing the uptime of critical business functions.

4.2.4. New Project Funding

One of the critical elements of any project proposal is its budget. It is a pivotal tool that will be used by several separate groups involved in the project. The project manager will use this budget to determine whether the project is on track; project personnel will use it as a guideline to fulfill certain project milestones; and the stakeholders will use it to determine the effort's success.

The CISO, as a business leader, requires accurate information to support financial decisions for the information security program. Decisions about capital investment are among the most

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

important.

The acquisition of long-term operational assets is a capital investment. The CISO should be aware of and plan to use these investments as part of the financial management strategy because capital asset investments can usually be recovered only using those assets. Once an organization purchases a capital asset, it is committed to that investment for an extended period. The organization experiences the consequences, including the inability to seize new opportunities, because the capital is invested. To a large extent, business profitability hinges on the quality of capital investment decisions.

Making the right financial decision [120]

Two primary characteristics distinguish relevant from useless information from a financial management perspective. First, relevant information differs among the alternatives for consideration. Costs that are similar among the alternatives are avoidable and, therefore, irrelevant. A second characteristic of pertinent information is that it is future-oriented, which means you cannot avoid a cost already incurred. In addition, relevance is context-sensitive. A cost that is relevant in one context may be irrelevant in another. Information can be vague to be relevant, but the most helpful information is relevant and precise.

To make the right decision, the CISO needs information. For example, comparing salaries for a SOC analyst and a helpdesk analyst is irrelevant because the skillsets are entirely different, and the roles are different. Several techniques are available to aid the CISO in comparing alternative capital investment opportunities. NPV, ROI, and Cost-Benefit Analysis (CBA) are the most appropriate techniques to compare options in a capital investment decision.

You are not necessarily at a standstill if your budget is frozen or reduced. Implement proof of concepts for new projects if you are still waiting to get them funded. Many vendors, especially those trying to establish a market presence, are willing to conduct free Proof of Concept (POC) projects, like a test drive of a new project management system, to establish presence for when the budget becomes available. One of the best ways for them to do this is to demonstrate the value of their products in a POC—not only to you but to others in the business who will also benefit. If the POC is successful, you might garner additional funding support. A POC also allows you and your company to observe a vendor and their behaviors. This allows you to determine if the vendor represents a company you can work with and trust.

4.2.5. Contingency Funding

- **Cryptocurrency Wallet:** If an organization decides to pay a ransom request resulting from a ransomware attack, having a cryptocurrency wallet is prudent. Establishing a wallet during an event could take days. With many options, including Bitcoin, Ethereum, and other cryptocurrency wallets available [121], deciding can be challenging. How much an organization places in the wallet depends on its size. One recent ransomware payment demand was $70 million (NetApp, 2022).
- **Disaster Declarations:** If an organization uses a contracted disaster recovery facility, a disaster declaration fee is often required to activate the site. Declaration fees vary, depending on the organization's recovery contract size. Out-of-pocket expenses incurred by the Go team also need to be accounted for, consisting of the first responders who go to the recovery site or other locations to resume critical processing. Go team members will require reimbursement of travel expenses. CISOs should work

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

with their Disaster Recovery (DR) teams to obtain disaster declaration estimates and then work with their CFO to provide for these costs during a disaster event.

- **License Creep:** It is common for security technology licenses to increase over time. For example, the number of monitored events per second could dramatically increase, quickly surpassing the license limits of a Security Information and Event Management (SIEM) product. Increases in new hires could increase the per-seat charge for endpoint security software. CISOs should consider these and other potential budget-impacting scenarios.

4.3. Managing the information Security Budget

Budget management involves analyzing and overseeing the costs and expenditures of the information security program. Managing an information security budget requires that CISOs adhere to their organization's financial management protocols. A well-managed information security program budget allows for smooth operations, growth, and recognition of the CISO as a competent steward of organizational funds.

Budgets sometimes go differently than envisioned. Numerous factors can impact the information security budget, necessitating tough decisions by the CISO. A CISO should prioritize their budget so they know what could be cut if their budget is unexpectedly reduced. The best way to accomplish this is to identify which budget items represent discretionary spending. Discretionary does not necessarily mean unimportant; it just means that these items can be delayed, or less costly options may exist. Work with the organization's CFO to find creative ways to adjust the information security program budget. For example, shifting a CapEx to an OpEx expense may help.

CISOs can refine budget estimates by considering some basic economic principles:

- Today's dollar is worth more than tomorrow due to favorable interest rates (discount rate) and inflation.
- Inflation and foreign exchange rates are externalities and macroeconomic factors that are not in the control of the company management.
- Not all resources are the same. The opportunity cost of a resource allocated or committed for a project must be considered. The opportunity cost of a choice is the value of the best alternative forgone.
- Price movements are influenced by supply, demand, and substitute forces. Prices increase if supply declines, demand grows higher, or a substitute becomes unavailable.
- A sunk cost is money that has already been spent and cannot be recovered. The sunk cost fallacy (or lost cost trap) is a cognitive bias that causes people to stick with a plan, course, or approach, even when it is failing.
- Switching costs are hidden or sometimes forgotten. Switching costs are the costs a consumer incurs because of changing brands, products, service providers, or suppliers.
- Financial management requires quantifying intangibles. Though CISOs often detail the value and significance of intangible assets in qualitative descriptions, they can quantify them for budgeting and financial planning. Information security quality reputation, cost of rework quality, preventing regulation fines, customer retention and positive reviews, and skilled (information security) employee retention can be quantified and detailed in the

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

budget proposals.

4.3.1. Obtain Financial Resources

The information security program can be funded from several sources and understanding these sources can help structure the budget. Sources can include department chargeback, vendor financing, value-added service charges, or a marketing subsidy.

- **Capitalization:** This method leverages the U.S. Securities and Exchange Commission (SEC) accounting standings for capitalizing technology costs. CISOs should discuss with their CFO to use the following SEC's Accounting Standards Codification (ASC):
  - **ASC 350-40: Internal Use Software:** This provision may allow the expense of some of the cost of cybersecurity software used to protect internal systems. This would include intrusion detection systems, firewalls, and antivirus.
  - **ASC 605-50: Customer Payments and Incentives:** This rule may allow you to expense the cost of data breach customer retention costs consisting of credit monitoring subscriptions, customer security software, and other qualifying investments.
  - **ASC 450-20: Loss Contingencies:** This rule may allow you to deduct probable and estimated losses from a cyberattack.
- **Chargeback:** This method is where the costs of running the information security program are evenly distributed to each department based on the number of users. This is ideal for mandatory security services such as email filtering and antimalware.
- **Marketing Subsidy:** Today, organizations can improve their market position with improved security. This creates a value that marketing departments may be willing to invest in if they feel they can monetize the information security program into increased product sales.
- **Value-Add Service Pricing:** Today, many CISOs structure their information security program as services with accompanying service levels. Base service levels are paid for through chargeback; however, the requesting department pays higher service levels at cost. For example, application security scanning is specific to an application, so the application owner should pay for that cost.
- **Vendor Financing:** This is a method where the service provider or technology vendor provides financing. This materializes as an OpEx to your budget rather than a CapEx. Many vendors offer unique financing options to market their products.

4.3.2. Allocate Financial Resources

Allocating financial resources is among the most challenging decisions a CISO must make. Giving too little or too much into a service specific can misalign the security program with the organization's risk profile. The CISO should pursue a risk-based approach to allocating their budget to ensure the most critical areas of the organization are adequately protected.

The following study of the state of IT spending on information security produced by Spiceworks provides insight as to how other companies are allocating their information security dollars. In their 2018 survey, North American and European respondents stated how much of a category was spent on information security [122]. The following are the top four categories where information security dollars were allocated in 2018:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

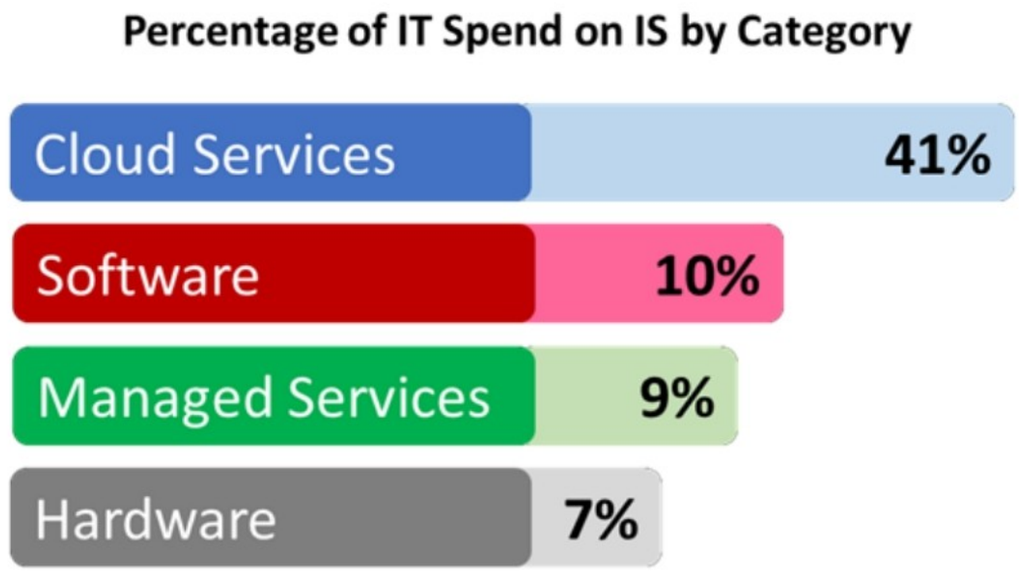


Figure 72: Information Security Spending Percentage by IT Category

4.3.3. Monitor and Oversight of Information Security Budget

Monitoring an information security program budget and overseeing spending requires transparency, which results in accountability by the information security program management. CISOs need to show that information security program funding is spent effectively according to its stated purpose. Every dollar of the budget needs to be accounted for, and the initially stated value of each funding request business case needs to be tracked. For example, if $250,000 was provided for endpoint security, was risk reduced by the percentage presented? Oversight needs to show value to sponsors and stakeholders on a continual basis.

4.3.4. Report Metrics to Sponsors and Stakeholders

One way to show transparency is to report financial metrics of the information security program, specifically. Deciding which financial metrics to use is part art and part science, as ROI is difficult to show for something intangible (such as security). Regardless of the difficulty, a CISO needs to report financial metrics. One of the best ways is to create a spending baseline and show improvement over time. Another way is to compare the cost of providing various information security services in-house versus outsourced offerings.

The following are several metrics that many CISOs find compelling:

- **Cost Per Seat:** Showing the cost of the information security program broken down by cost per individual user places things in perspective for most CFOs, sponsors, and stakeholders. For example, if your organization spends $75,000 annually on antivirus software for 1,400 users, the cost is approximately $4.50 monthly per user. CISOs should have every information security service in their portfolio cost by the users to produce these metrics.
- **Internal versus External Service Cost:** CISOs should always look to see if the services provided by their information security program are comparable and cost-competitive with the benefits of managed service providers. At least annually, a comparison should be made and reported on to present to management the cost of providing security services in-house. CISOs should always be open to switching if a business case supports moving toward an external service provider.

4.3.5. Balancing the Information Security Budget

As the CISO for your organization, you must produce a balanced budget annually. You must show that your information security program's expenses do not exceed its investment. A

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

balanced budget will demonstrate to senior management that you effectively manage the organization's investment. Balancing a budget requires careful attention to monthly spending and making tough decisions to reduce spending if the budget becomes out of balance.

5. PROCUREMENT

We have all heard stories of ethical lapses in procurement, many of which involve the procurement of technology. To ensure adherence to the organization's purchasing policies, it is essential to understand how the process works. Procurement is a finance discipline integral to how organizations source and acquire goods and services. CISOs must understand how their organization purchases to manage the information security program effectively. Purchasing is a core management knowledge area in which CISOs should be proficient.

5.1. Procurement Program Terms and Concepts

The fundamentals of purchasing are the foundation of the purchasing department, which is a crucial part of the business. There are several ways purchasing is managed within organizations.

5.1.1. Statement of Objectives (SOO)

The Statement of Objectives (SOO) is part of an RFP from the U.S. Government. The SOO is an alternative to a government-prepared statement of work. A SOO provides the government's overall objectives and specifies the support required from the offeror to achieve these contractual objectives.

hide01.ir

5.1.2. Statement of Work (SOW)

A Statement of Work (SOW) is a document that defines the scope of a project, specific deliverables, scheduling, and additional responsibilities as required by the purchasing company. A SOW is a binding contract between two parties more specialized in scope, language, and deliverables (as opposed to a Request for Proposal (RFP)).

5.1.3. Total Cost of Ownership (TCO)

Total Cost of Ownership (TCO) is a financial estimate to help buyers and owners determine a product or system's direct and indirect costs. This management accounting concept, including social costs, can be used in full-cost accounting or ecological economics. In measuring ROI or total value of an asset over its full-term lifecycle, it is essential to consider ongoing operational or maintenance costs and any other hidden costs in addition to initial purchasing (or direct) costs.

5.1.4. Request for Proposal (RFP)

The Request for Proposal (RFP) is considered a best practice designed to assist in procuring services. RFP is beneficial because it facilitates a bidding process that may drive down prices or increase value as vendors compete to win bids. Processes used to create an RFP should outline the bidding process and contract terms and guide the bid formatting and presentation. This presents an excellent opportunity for the organization facilitating the RFP to include security requirements in the proposal and evaluate the capability of vendors to meet those requirements.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5.1.5. Request for Information (RFI)

Related to the RFP process is an activity known as Request for Information (RFI), which provides the opportunity to collect information about a supplier's capabilities. This approach is used when an organization needs more details before asking for an RFP. Instead, the organization uses the RFI process to learn about vendor capabilities and then chooses a vendor who can work with the organization for the solution.

5.1.6. Master Service Agreement (MSA)

A Master Service Agreement (MSA) is a contracting artifact that details the responsibilities and obligations of two parties to each other. MSAs are the general operating rules for all contracts. Rates and terms are found in the individual contracts. MSAs provide guiding legal requirements for all contracts and services. Subordinate agreements like SLAs, purchasing agreements, purchase orders, and SOWs offer additional details.

5.1.7. Service Level Agreement (SLA)

A service level agreement (SLA) is a contract that defines the quality and volume of specific deliverables and levels of services delivery requirements for both parties. A comprehensive SLA will include performance metrics to ensure both parties' expectations are met throughout the contract lifecycle. SLAs must have consequences, penalties, or alternative options when the involved parties fail to fulfill their obligations.

5.1.8. Terms and Conditions (T&C)

Terms and Conditions (T&C) are rules and guidelines that users must agree to use a product or service. It acts as a legal contract between you (the company), and the owner of the technology or deliverer of the services.

It is up to you to set the rules and guidelines that the user must agree to. An example of this is a T&C agreement representing the legal agreement whereas you maintain your rights to exclude consumers from using your application if they abuse it.

Terms and Conditions are also known as Terms of Service or Terms of Use.

CISOs must consult their organization's legal and procurement teams when reviewing the documents above to ensure standard and appropriate language is used within them

5.2. Understanding the Organization's Procurement Program

The traditional purchasing process involved several steps—requisition, soliciting bids, purchase order, shipping advice, invoice, and payment—that have come to be increasingly regarded as unacceptably slow, expensive, and labor intensive. Each transaction generated its paper trail, and the same process is followed regardless of what is being purchased.

5.2.1. Internal Policies, Processes, and Requirements

Organizations will have policies, procedures, and processes to guide CISOs in procuring information security products and services. These must be read and understood. Some of the terms CISOs will encounter are as follows:

- **Procurement Limits:** This is a limit of procurement preauthorized for a department or individual, typically referred to as signing authority. This is how much an individual can spend without additional approvals.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Procurement Authority:** This is the designation of who within the organization has the authority to make a purchase or issue an RFP. A dollar amount is typically used to grant authority.
- **Formal Bidding:** This is the process where an organization issues a tender or bid for the resulting purchase of a product or service. The common vehicle for this is an RFP.
- **Informal Bidding:** This is a process where a select group of companies are invited to openly bid for products or services.
- **Bid Requirements:** These are the requirements an organization wants, at a minimum, for a company to submit in response to an RFP.
- **No Bid:** Sometimes, vendors will not bid on an RFP because they feel the customer requirements are too strict, the product or service requirements are not a match, or the RFP has been written specifically to exclude their company.
- **Sole Source:** This is a situation where the organization does not require multiple companies to bid. This is common in times of emergency or where an existing provider is trusted to rapidly provide the needed products or services.
- **Piggyback Contracts:** These are previously bid contracts typically awarded within the past 12 months. An organization can use the same contract to acquire goods or services for the same or lower pricing.
- **Vendor Requirements:** This is where organizations can specify criteria that a vendor must meet. This could include years in business, financial health, incorporation location, and number of customers.
- **Sealed Bid:** The RFP response is submitted without competing vendors knowing what was submitted.
- **Public Bid Opening:** Participants of a sealed bid process might be permitted to hear initial bids in a public forum.
- **Contesting a Bid:** If a vendor believes the bid had restrictive specifications, omission of required revisions, or ambiguous evaluation factors, they can challenge a competitor's award of a contract.
- **Preferred Vendor:** A preferred vendor refers to a trusted supplier that has been vetted or approved and chosen by a company to provide goods or services to that company on an ongoing basis. Preferred vendors add value to the company's supply chain as they can optimize efficient business operations, enhance risk management, and contribute to cost savings.

5.2.2. External or Regulatory Requirements

Most of us have read or heard reports of at least one of the instances where an organization's procurement process was riddled with fraud. Several legal requirements have evolved to prevent fraud or collusion in the procurement process. CISOs must understand that improper and fraudulent procurement actions can lead to dismissal or arrest. Public organizations have strict legal requirements for procurement; however, public and private organizations can be bound by laws that dictate how a company should conduct procurement operations.

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CISOs need to understand the following external and regulatory aspects of procurement:

- **Commercial Bribes:** Many jurisdictions have strict laws against offering bribes or kickbacks in procurement. Government organizations are the toughest in prohibiting bribes. CISOs must report any situation where a vendor has provided something in return for choosing their product or service.
- **Ethics:** Ethics is a standard by which someone must conduct themselves in the procurement process.
- **Disadvantaged Organization Procurement:** Government organizations often provide preference for a certain amount of their procurements to what is referred to as 8(a) companies. These include small, disadvantaged, minority-owned, women-owned, and veteran-owned businesses.
- **Uniform Commercial Code (UCC):** This is the law of sales and other commercial transactions within the United States. The UCC protects purchasers in that products or services acquired should have a warranty of fitness for a particular use. The UCC typically does not cover service contracts.

5.2.3. Local Versus Global Requirements

It has become widespread practice to offshore security services to low-cost locations. Global resourcing of information security has been less popular in the recent past due to data residency or storing sensitive data outside of the country of origin. Accessing a home county's data from a foreign country by an offshore team may be discouraged by local regulations such as the California Consumer Privacy Act (CCPA), the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, General Data Protection Regulation (GDPR) of European Union, and the Law of General Personal Data Protection (LGPD) of Brazil. In some parts of the world, the practice is more commonplace.

5.3. Procurement Risk Management

Procurement demands the highest integrity regardless of whether an organization is public or private. Irregularities in the purchasing process or even the appearance of impropriety can invalidate the entire process. As the CISO, you must ensure that your department is not the cause of fraud, vendor favoritism, or conspiracy. The goal of a CISO is to abide by the organization's procurement policies to avoid errors or policy inconsistencies. Anything less can lead to accusations that, even if proved to be without merit, could damage the reputation of the CISO and the information security program.

One effective method is to perform a periodic risk assessment of how the information security program procures products and services. This can be useful for identifying potential issues with procurement activities within the security function.

The following procurement risk checklist will help identify your department's compliance with procurement policies:

- Are products or services acquired with a transparent and fair RFP process?
- Do members of the information security team socialize (including meals) with vendors?
- Are purchasing decisions influenced by exceptional circumstances, such as end-of-year pricing?

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Are internal control systems capable of ensuring compliance with the legal and regulatory requirements?
- Are procurement decisions well documented and available for audit?
- Are RFPs comprehensive, transparent, and free from restrictions or conditions that would unduly discriminate against certain vendors?
- Was timely and equal access to contract documents and information provided to interested potential vendors?
- Was adequate time taken for consideration of proposals before being awarded to a vendor?
- Was the award decision process accurate and adequately communicated?

5.3.1. Standard Contract Language

A company must know and understand the contents of its contracts. A company must know which contracts require the inclusion of language about data protection and the management of security breaches. This will ensure that the company knows what actions may be required or what actions it may expect of the other party in the event of a breach.

For example, if a company does not know if it has contracts that contain breach-related language and requirements, then in the event of an attack the vendor may fail to notify customers of the breach or fail to take other action. Alternatively, a company may need to legally define the actions the other party to a contract must take if that party suffers a breach. A lack of clear contract language may make it difficult to hold the offending party accountable.

A breach combined with one party's failure to take the contractually required action may worsen an already complicated and expensive situation. Companies can reduce the potential impact of unforeseen events by understanding their contract portfolio, particularly the clauses and provisions related to significant occurrences (such as a cyberattack).

6. VENDOR MANAGEMENT

Organizations often use vendors to support operations and activities. Vendors can add or enhance capabilities that produce positive organizational results. Organizations must evaluate and understand the risks presented by vendor relationships. From a security perspective, the primary reason for performing vendor management is to understand the risk a vendor will introduce to or mitigate for the organization. To achieve effective vendor management, the CISO should work with the organization to ensure vendor risks are understood, policies and standards are defined to address those risks, and processes exist to monitor vendors for performance and security compliance.

Effective risk management is critical when an organization uses a third party, such as a managed security service provider (MSSP), to support risk management and risk treatment activities. Although the vendor provides a valuable service, the arrangement adds another component to the risk management matrix because the vendor supporting risk management also must be managed.

Two distinct phases are used to support vendor risk management activities: procurement and vendor management.

6.1. Understanding the Organization's Acquisition Policies and Procedures

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Procurement Life Cycle

The procurement phase of vendor risk management focuses on the organization's steps before the relationship with the vendor begins. Effective vendor management starts with the procurement process.

The procurement life cycle consists of various phases depending on the maturity and the organization's needs. Common considerations include planning, vendor assessment and selection, contract negotiation, and performance management.

Figure 73: Vendor Procurement Cycle

- **Planning:** Planning is a critical prerequisite for effective vendor risk management. Organizations assume significant risk by approaching vendor management without an appropriate plan. Planning starts by outlining specific policies to define requirements for all procurement activities within an organization. The CISO is rarely responsible for leading the procurement effort; however, the CISO's participation in this effort has considerable influence on the outcome. The CISO should collaborate with organizational leaders and legal counsel to identify the standards required in contracts and the language needed to achieve those standards. For example, many organizations define security and privacy clauses that apply to all contracts to ensure consistency across all vendors or services.
- **Vendor Assessment and Selection:** The Request for Proposal (RFP) is regarded as a best practice designed to assist in procuring services. An RFP is beneficial because it facilitates a bidding process that may drive down prices or increase value as vendors compete to win bids. Processes used to create RFPs should outline the bidding process and contract terms and guide how the bid should be formatted and presented. This presents an excellent opportunity for the organization facilitating the RFP to include security requirements in the proposal and evaluate the capability of vendors to meet those requirements.
- **Contract Negotiation:** Contract negotiation is a vital component of vendor management. Key stakeholders representing everyone affected by the contract should be involved in evaluating the vendor's terms, expectations, and requirements. This provides opportunities to ensure usability, which is essential from the organization's perspective. Contract

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

negotiation is considered a governance activity. The organization should establish a governance board to review contracts and ensure requirements are met from multiple organizational perspectives. This promotes corporate collaboration.Contract negotiation should seek to optimize the contract details for the organization's best possible outcomes. Crucial factors to consider during this phase include:

- **Indemnity:** The negotiation should agree on which party assumes responsibility for security incidents and penalties related to such an event.
- **Security:** The negotiation should establish an agreement about the security controls the vendor agrees to implement and manage for compliance and risk management.
- **Audit:** The negotiation should establish an agreement about the level of access an organization will have to audit the vendor's controls or environment.

If the organization and the vendor cannot agree to the terms, it may be best not to sign the contract. Organizations must weigh trade-offs between the value of the service offered by the vendor and the risk the organization assumes by doing business with the vendor.

Four groups are critical to evaluating and approving contracts during the negotiation phase.

- **Legal:** The legal team is a critical partner in any contract review because contracts are legal agreements that require specialized skills and knowledge.
- **Security:** Subject Matter Experts (SMEs) and leadership from the security program must review the contract and guide information security, audit, and compliance requirements.
- **Executives and Organizational Leaders:** Executives and organizational leaders have a stake in the outcome of all contracts, whether from a financial or administrative perspective. These stakeholders are critical participants in contract governance because they have the power to influence the negotiation.
- **Users:** A representative from the group who will use the product or service obtained by the procurement should participate in the contract review. This group is best positioned to evaluate the solution's usability.
- **Performance Management:** The ability to formally define expectations and hold vendors contractually accountable is one of the benefits of using third parties to support the organization. Artifacts from the contract will clearly define the expectations of the organization and the vendor. Once complete, the organization and the vendor can use these artifacts to measure performance. Large organizations with numerous vendors often establish a vendor management office to oversee and monitor vendors according to the agreements set in the contracts at procurement.

The most common artifacts to define the work to be delivered include the Master Service Agreement (MSA), Service Level Agreement (SLA), and Statement of Work (SOW).

6.2. Applying Cost-Benefit Analysis (CBA) During the Procurement Process

Cost-benefit analysis (CBA) provides the most straightforward calculation among financial comparison tools but is the least precise. This model is often used to produce quick comparisons of two options.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The outcome of a CBA comparison will help determine whether a project is financially feasible and desirable or another project should be pursued. CBA analyzes decisions by identifying the benefits of a decision in terms of total value and subtracting the costs associated with taking that action.

Total Benefit – Total Cost = CBA

Unfortunately, calculations used to estimate the total benefit or value of an intangible asset or activity are difficult. Models that apply a monetary value to are often required to support this analysis. The organization must agree on the valuation model to provide a practical assessment. Like the other models, a positive result indicates that investment should be pursued and the investment with the highest CBA is optimal.

6.3. Vendor Management Policies

A set of policies specifically designed to communicate how your organization treats and manages a third-party relationship is essential for proper vendor management.

The third-party policy should cover, at a minimum:

- **Monitoring**: This policy describes how the relationship will be monitored and at what frequency.
- **Change Management:** This policy outlines the procedure for requesting, approving, and documenting a change to contracts.
- **Change in Ownership/Management:** This policy requires the third party to notify the organization when key management or delivery personnel are changed, or the provider has been acquired.
- **Material Change in Vendor Bid Requirements:** This policy requires notification in the event of a material change in the third party's financial condition, product certifications, or other changes as provided in bid requirements.
- **Risk Management:** This policy describes the process for performing a risk assessment of the services or products being contractually delivered.
- **Delivery Auditing:** This policy defines how delivery audits will be performed, exception management, and the frequency at which audits will be completed.
- **Incident Management:** This policy requires identified stakeholders to be notified if a breach of security or data loss is experienced by the third party, including confirmation of types and quantities of data involved in an incident.
- **Service Outage Reporting:** This policy requires notification of SLA failures resulting in a disruption to the provider or customer business operations beyond the allowable SLA limits due to service delivery or product failure.
- **Contract Closure**: This policy defines how the organization's sensitive information is treated at the termination of the agreement.

6.4. Contract Administration Policies

Contracts must be properly administered when dealing with third parties. This is critical with vendors providing security and continuity products and services to the organization.

nide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.4.1. Service and Contract Delivery Metrics

Establishing metrics aligned to the contracted product or service is essential for proper contract oversight. Commitments the vendor represents in the contract can be used to model metrics. Attainment of metrics can also be used to structure vendor payments. The Work Breakdown Structure (WBS) is typically used to define milestones by outlining what will be accomplished and within what timeframe. These structures can also be converted to percentage of completion metrics to structure payments and gauge the vendor's progress in meeting their contractual obligations.

6.4.2. Contract Delivery Reporting

Contract transparency includes reporting on contract performance. At times there can be a reluctance to report deficient performance by those who made the purchasing decision as it would reflect poorly on them. The CISO must have the integrity to report vendor performance regardless of whether the performance is good or bad. CISOs should accept that only some vendors will not deliver positive results despite applying due diligence. Transparent reporting helps others in the organization make better vendor selection decisions by learning from previous procurement decisions. Reporting should be targeted to the sponsors and stakeholders of the product or service.

6.4.3. Change Requests

Once a contract has been signed, any changes should only be made through a formal change request process. Verbal agreements should not be used as they could invalidate a contract or affect how the product or service is supported going forward. Contracts typically include a section detailing change processes.

ride01.ir

6.4.4. Contract Renewal

Contract renewal allows for improvements in price, service, delivery, or other contract aspects after the initial contract term occurs. Treating the contract renewal period can be viewed as establishing an entirely new contract, and at times is in the best interest of your organization. This is a chance to obtain the same incentives that new customers are offered or take advantage of creating a sole-source situation. Other aspects can also be reviewed. For instance, security policies might have changed, and those that apply to vendors should be considered for inclusion at renewal time. This process should begin prior to contract expiration and provide ample time to change providers if the organization cannot come to acceptable terms with the vendor.

6.4.5. Contract Closure

Ending a contract requires a close-out period. This is where all information previously provided, stored, or processed by the vendor is destroyed or returned to the organization. If a right-to-audit clause was inserted in the contract language, an audit should be performed to verify that all sensitive material has been reviewed. At a minimum, a certificate of destruction should be provided. A close-out meeting with the vendor or service provider should be held to cover any contract clauses beyond the agreement's active service portion. This would include reaffirming the confidentiality clause length, ceasing the use of the organization's name in marketing materials, and others as applicable. Contract closure is also the time to review the requirements of the organization, including the removal of all intellectual property and licenses and the return of any appliances [53].

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.5. Delivery Assurance

6.5.1. Validation of Meeting Contractual Requirements

A simple but effective method of managing vendors is to use a checklist. CISOs should create a checklist of vendor commitments outlined within contracts, SOWs, and WBSs. The checklist should identify obligations, dates of commitment fulfilment, the demonstration of proof of completion, and verifier information. Once completed, the checklist can be used as a baseline for a gap assessment between vendor commitments and performance.

6.5.2. Formal Delivery Audits

Auditing a vendor or service provider can take time and be expensive. Auditing may be part of the vendor selection process, annual compliance requirement, or contract closure. Some organizations have the resources to perform these audits, while others may outsource this function to an independent third party. The level of criticality the vendor has to an organization and the sensitivity of the information they interact with should dictate the level of audit detail required. This can range from completing detailed self-assessments to interviewing key personnel to conducting vulnerability scans or penetration testing.

6.5.3. Periodic Random Delivery Audits

One of the most difficult audits to negotiate and successfully execute is periodic random delivery audits. These differ from regularly scheduled annual audits due to their randomness. Few service providers or vendors will expose their operations and personnel to unannounced audits of their business. This type of audit is typically reserved for providers of large contracts involving high risk assets. The rules of engagement for random audits are negotiated in the initial contract.

6.5.4. Third-Party Attestation Services (TPRM)

The time and effort required for organizations to manage their TPRM programs has created an industry of service providers who independently assess and report on a third party's cybersecurity and regulatory status.

The following table provides examples of the more well-known providers of third-party assurance programs:

Program	Provider	Overview
AICPA SOC 2®	American Institute of CPAs	Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service
BSI Kitemark™ for Products	The British Standards Institution	BSI Kitemark scheme involves an initial assessment of conformity to the relevant standard and an assessment of the quality management system operated by the supplier

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CSA STAR Registry	Cloud Security Alliance (CSA)	Registry of over 100 cloud service providers who passed the CSA security assurance program
HITRUST Third- party Assurance Program	HITRUST Alliance	Third-party assurance program for healthcare IT service providers
ISO 27001 Certification	The British Standards Institution	Companies that have been certified compliant with the ISO 27001 standard
Shared Assessments Program	Santa Fe Group	Collaborative, global, peer community of practitioners working to assess third-party provider risk

Table 28: Third-Party Assurance Program Providers

7. SUMMARY

Domain 5 focuses on strategic planning, financial management, and vendor management as critical business-centric concerns related to effective leadership by the CISO.

Strategic planning is a business management discipline that focuses on the systematic processes of envisioning a desired future and defining processes to transform that vision into reality. The strategic plan communicates the priorities and objectives of the CISO's information security program. The strategy is measured by the effectiveness of planning, execution, and the requirements outlined in the strategy's KPIs.

Financial management defines the processes of planning, organizing, directing, and controlling the monetary activities of an organization and how funds are used. The CISO's execution of financial management principles will influence the stewardship of financial resources provided by the organization to support the information security strategy. Budgeting, expense management, and the tools used to compare capital investments contribute to successful financial leadership from the CISO.

Vendor risk management focuses on understanding the risk introduced by an organization's services and products providers. The procurement phase of vendor risk management focuses on the organization's steps before the relationship with the vendor begins. Defining security language that supports the organization's risk management goals is procurement's most crucial security objective. This language should be incorporated into the RFP and other documentation used to support the acquisition of services and products. Vendor management focuses on the activities an organization must perform after the vendor agreement is approved and delivery begins.

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.
hide01.ir

References

[1] "Corporate Governance: Definition, Principles, Models, and Examples." Accessed: Nov. 04, 2023. [Online]. Available: https://www.investopedia.com/terms/c/corporategovernance.asp

[2] "The nature of the CISO role will be in flux in 2023 | Computer Weekly." Accessed: Nov. 04, 2023. [Online]. Available: https://www.computerweekly.com/news/252528303/The-nature-of-the-CISO-role-will-be-in-flux-in-2023

[3] "LAW Definition & Usage Examples | Dictionary.com." Accessed: Nov. 04, 2023. [Online]. Available: https://www.dictionary.com/browse/law

[4] "Code Of Ethics | EC-Council." Accessed: Nov. 04, 2023. [Online]. Available: https://www.eccouncil.org/code-of-ethics/

[5] "Risk management - Wikipedia." Accessed: Nov. 04, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Risk_management

[6] "SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/30/r1/final

[7] "SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/37/r2/ipd

[8] "SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/39/final

[9] "ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/75281.html

[10] "ISO - ISO 31000 — Risk management." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/iso-31000-risk-management.html

[11] "The Essentials of Risk Management, Third Edition." Accessed: Nov. 04, 2023. [Online]. Available: https://www.mhprofessional.com/the-essentials-of-risk-management-third-edition-9781264258864-usa

[12] "ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/80585.html

[13] "About Us | COSO." Accessed: Nov. 04, 2023. [Online]. Available: https://www.coso.org/about-us

[14] "FAIR Methodology for Quantifying Information Risk." Accessed: Nov. 04, 2023. [Online]. Available: https://www.fairinstitute.org/about

[15] "Factor analysis of information risk Jones, Jack A. [Jones, Jack A.]." Accessed: Nov. 04, 2023. [Online]. Available: https://uspto.report/patent/app/20050066195

[16] "Lean Risk Assessment based on OCTAVE Allegro – Compass Security Blog." Accessed: Nov. 04, 2023. [Online]. Available: https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

[17] "(PDF) Prioritizing Information Security Risks with Threat Agent Risk Assessment (TARA)." Accessed: Nov. 04, 2023. [Online]. Available: https://www.researchgate.net/publication/335589639_Prioritizing_Information_Security_Risks_with_Threat_Agent_Risk_Assessment_TARA

[18] "HITRUST Alliance | HITRUST CSF | Information Risk Management." Accessed: Nov. 04, 2023. [Online]. Available: https://hitrustalliance.net/product-tool/hitrust-csf/

[19] [20] "ISO - The ISO Survey." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/the-iso-survey.html

[21] "ITIL | IT Service Management | Axelos." Accessed: Nov. 04, 2023. [Online]. Available: https://www.axelos.com/certifications/itil-service-management

[22] "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 | NIST." Accessed: Nov. 04, 2023. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[23] "SP 800-53A Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/a/r4/upd1/final

[24] "Federal Information Security Modernization Act | CISA." Accessed: Nov. 04, 2023. [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

[25] "HIPAA for Professionals | HHS.gov." Accessed: Nov. 04, 2023. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/index.html

[26] "HITECH Act Enforcement Interim Final Rule | HHS.gov." Accessed: Nov. 04, 2023. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

[27] "FAQ - GDPR.eu." Accessed: Nov. 04, 2023. [Online]. Available: https://gdpr.eu/faq/

[28] "Information Security Manual (ISM) | Cyber.gov.au." Accessed: Nov. 04, 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

[29] "Basel III: international regulatory framework for banks." Accessed: Nov. 04, 2023. [Online]. Available: https://www.bis.org/bcbs/basel3.htm

[30] "FFIEC Cybersecurity Awareness." Accessed: Nov. 04, 2023. [Online]. Available: https://www.ffiec.gov/cyberassessmenttool.htm

[31] "ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/contents/data/standard/05/45/54534.html

[32] "ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/75652.html

[33] "ISO/IEC 27003:2017 - Information technology — Security techniques — Information security management systems — Guidance." Accessed: Nov. 04, 2023. [Online]. Available:

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://www.iso.org/standard/63417.html

[34] "ISO/IEC 27004:2016 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/64120.html

[35] "ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/74046.html

[36] "ISO/IEC TR 27016:2014 - Information technology — Security techniques — Information security management — Organizational economics." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/43756.html

[37] "ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/43757.html

[38] "ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/76559.html

[39] "ISO/IEC 27032:2023 - Cybersecurity — Guidelines for Internet security." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/76070.html

[40] "ISO/IEC 27034-1:2011 - Information technology — Security techniques — Application security — Part 1: Overview and concepts." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/44378.html

[41] "ISO/IEC 27035-1:2023 - Information technology — Information security incident management — Part 1: Principles and process." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/78973.html

[42] "ISO/IEC 27036-1:2021 - Cybersecurity — Supplier relationships — Part 1: Overview and concepts." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/82905.html

[43] "ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/44381.html

[44] "Reliability Standards." Accessed: Nov. 04, 2023. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

[45] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards." Accessed: Nov. 04, 2023. [Online]. Available: https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss

[46] "SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

[47] "SP 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies | CSRC."

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/40/r3/final

[48] "SP 800-50 Rev. 1, Building a Cybersecurity and Privacy Learning Program | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/50/r1/ipd

[49] "SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/ipd

[50] "SP 800-55 Rev. 1, Performance Measurement Guide for Information Security | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/55/r1/final

[51] "SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final

[52] "SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final

[53] "SP 800-88 Rev. 1, Guidelines for Media Sanitization | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/88/r1/final

[54] "SP 800-114 Rev. 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/114/r1/final

[55] "SP 800-125, Guide to Security for Full Virtualization Technologies | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/125/final

[56] "SP 800-137A, Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/137/a/final

[57] "SP 800-160 Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/160/v1/upd2/final

[58] "SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/181/final

[59] "AICPA SSAEs – currently effective | Resources | AICPA & CIMA." Accessed: Nov. 04, 2023. [Online]. Available: https://www.aicpa-cima.com/resources/download/aicpa-ssaes-currently-effective

[60] "CIS Critical Security Controls." Accessed: Nov. 04, 2023. [Online]. Available: https://www.cisecurity.org/controls

[61] "OWASP Top 10:2021." Accessed: Nov. 04, 2023. [Online]. Available: https://owasp.org/Top10/

[62] "ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/cms/%20render/live/en/sites/isoorg/contents/data/standard/08/28/82875.html

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

[63] "ISO/IEC 27007:2020 - Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/77802.html

[64] "ISO 19011:2018 - Guidelines for auditing management systems." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/70017.html

[65] "ISO/IEC TS 27008:2019 - Information technology — Security techniques — Guidelines for the assessment of information security controls." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/67397.html

[66] "COBIT | Control Objectives for Information Technologies | ISACA." Accessed: Nov. 04, 2023. [Online]. Available: https://www.isaca.org/resources/cobit

[67] "National Vulnerability Database (NVD) | NIST." Accessed: Nov. 04, 2023. [Online]. Available: https://www.nist.gov/programs-projects/national-vulnerability-database-nvd

[68] "HIMSS Healthcare and Cross-Sector Cybersecurity Report | HIMSS." Accessed: Nov. 04, 2023. [Online]. Available: https://www.himss.org/resources/himss-healthcare-and-cross-sector-cybersecurity-report

[69] "Resolving Conflict Situations | People & Culture." Accessed: Nov. 04, 2023. [Online]. Available: https://hr.berkeley.edu/hr-network/central-guide-managing-hr/managing-hr/interaction/conflict/resolving

[70] "Chief Information Officer - U.S. Department of Defense." Accessed: Nov. 04, 2023. [Online]. Available: https://dodcio.defense.gov/

[71] "Security Architecture | opengroup.org." Accessed: Nov. 04, 2023. [Online]. Available: https://www.opengroup.org/forum/security/architecture

[72] "The SABSA Institute - Enterprise Security Architecture." Accessed: Nov. 04, 2023. [Online]. Available: https://sabsa.org/

[73] "ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/75106.html

[74] "ISO/IEC 27031:2011 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/44374.html

[75] "ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/75107.html

[76] "ISO/TS 22318:2021 - Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/79001.html

[77] "ISO/TS 22317:2021 - Security and resilience — Business continuity management systems — Guidelines for business impact analysis." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/79000.html

[78] "SP 800-86, Guide to Integrating Forensic Techniques into Incident Response | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/86/final

hidee1.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

[79] "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [including updates as of 1-03-2018] | NIST." Accessed: Nov. 04, 2023. [Online]. Available: https://www.nist.gov/publications/systems-security-engineering-considerations-multidisciplinary-approach-engineering-0

[80] "A Quick Guide to Effective SIEM Use Cases." Accessed: Nov. 04, 2023. [Online]. Available: https://securityintelligence.com/posts/quick-guide-to-siem-use-cases/

[81] "Information Sharing and Analysis Centers (ISACs) — ENISA." Accessed: Nov. 04, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[82] "Federal Register :: Critical Foundations: Protecting America's Infrastructures." Accessed: Nov. 04, 2023. [Online]. Available: https://www.federalregister.gov/documents/1997/11/25/97-30851/critical-foundations-protecting-americas-infrastructures

[83] "SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/115/final

[84] "ThreatHunting Home." Accessed: Nov. 04, 2023. [Online]. Available: https://www.threathunting.net/

[85] "SP 800-63-2, Electronic Authentication Guideline | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/63/2/final

[86] "CI & Security Governance / Regulations." Accessed: Nov. 04, 2023. [Online]. Available: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-ci-security-governance-regulations

[87] "Forensic Science Laboratories: Handbook for Facility Planning, Design, Construction, and Relocation. | NIST." Accessed: Nov. 04, 2023. [Online]. Available: https://www.nist.gov/publications/forensic-science-laboratories-handbook-facility-planning-design-construction-and

[88] "ISO/IEC 27033-1:2015 - Information technology — Security techniques — Network security — Part 1: Overview and concepts." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/63461.html

[89] "ISO/IEC 27033-2:2012 - Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/51581.html

[90] "ISO/IEC 27033-3:2010 - Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/51582.html

[91] "ISO/IEC 27033-4:2014 - Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/51583.html

[92] "ISO/IEC 27033-5:2013 - Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/51584.html

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

[93] "ISO/IEC 27033-6:2016 - Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/51585.html

[94] "OWASP Mobile Application Security | OWASP Foundation." Accessed: Nov. 04, 2023. [Online]. Available: https://owasp.org/www-project-mobile-app-security/

[95] "SP 800-124 Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/124/r1/final

[96] "Mobile Device Security NIST SP 1800-4 Practice Guide Final | NCCoE." Accessed: Nov. 04, 2023. [Online]. Available: https://www.nccoe.nist.gov/publications/practice-guide/mobile-device-security-nist-sp-1800-4-practice-guide-final

[97] "Cross-Industry Insight: IoT Market Opportunities and Top Spend Use Cases." Accessed: Nov. 04, 2023. [Online]. Available: https://www.gartner.com/en/documents/4432199

[98] "3 Ways Blockchain Is Revolutionizing Cybersecurity." Accessed: Nov. 04, 2023. [Online]. Available: https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/?sh=4b884bf72334

[99] "SP 800-125A, Security Recommendations for Hypervisor Deployment on Servers | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/125/a/final

[100] "SP 800-125B, Secure Virtual Network Configuration for Virtual Machine (VM) Protection | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/125/b/final

[101] "2017 State Of Cloud Adoption And Security." Accessed: Nov. 04, 2023. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/?sh=32e83c9e1848

[102] "Top Threats to Cloud Computing Plus: Industry Insights | CSA." Accessed: Nov. 04, 2023. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-cloud-computing-plus-industry-insights/

[103] "Cloud Controls Matrix v3.0.1 ISO Reverse Mapping | CSA." Accessed: Nov. 04, 2023. [Online]. Available: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1-iso-reverse-mapping/

[104] "Cloud Customer Architecture for Securing Workloads on Cloud Services | Object Management Group." Accessed: Nov. 04, 2023. [Online]. Available: https://www.omg.org/cloud/deliverables/cloud-customer-architecture-for-securing-workloads-on-cloud-services.htm

[105] "AI Cyber Security Could Stop Hackers | WIRED." Accessed: Nov. 04, 2023. [Online]. Available: https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/

[106] "Who Says Software-Defined Security Is What We Want?" Accessed: Nov. 04, 2023. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2017/12/21/who-says-software-defined-security-is-what-we-want/?sh=201693fd7780#533523517780

[107] "Why Strategic Planning is More Important than Ever for Non-Profits | OnStrategy

hidoit.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Resources." Accessed: Nov. 04, 2023. [Online]. Available: https://onstrategyhq.com/resources/why-strategic-planning-is-more-important-than-ever-for-non-profits/

[108] "4.-Developing Your Strategic Plan - McNamara Carter | PDF | Strategic Planning | Strategic Management." Accessed: Nov. 04, 2023. [Online]. Available: https://www.scribd.com/document/228153755/4-Developing-Your-Strategic-Plan-McNamara-Carter

[109] "SEC.gov | Beginners' Guide to Financial Statement." Accessed: Nov. 04, 2023. [Online]. Available: https://www.sec.gov/reportspubs/investor-publications/investorpubsbegfinstmtguide

[110] "Crafting an Information Security Program Strategy | EDUCAUSE Review." Accessed: Nov. 04, 2023. [Online]. Available: https://er.educause.edu/blogs/2018/5/crafting-an-information-security-program-strategy

[111] "Strategic Planning Basics - Balanced Scorecard Institute." Accessed: Nov. 04, 2023. [Online]. Available: https://balancedscorecard.org/strategic-planning-basics/

[112] "Balanced Scorecard Basics - Balanced Scorecard Institute." Accessed: Nov. 04, 2023. [Online]. Available: https://balancedscorecard.org/bsc-basics-overview/

[113] "SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations | CSRC." Accessed: Nov. 04, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/137/final

[114] "Federal Enterprise Architecture Framework Version 2 - The EA Pad." Accessed: Nov. 04, 2023. [Online]. Available: https://eapad.dk/gov/us/feaf2/

[115] "What is the Zachman Framework? A matrix for managing enterprise architecture | CIO." Accessed: Nov. 04, 2023. [Online]. Available: https://www.cio.com/article/193229/what-is-the-zachman-framework-a-matrix-for-managing-enterprise-architecture.html

[116] "The Framework for Enterprise Architecture: Background, Description and Utility - Zachman International - FEAC Institute." Accessed: Nov. 04, 2023. [Online]. Available: https://zachman-feac.com/the-framework-for-enterprise-architecture-background-description-and-utility

[117] "TOGAF | opengroup.org." Accessed: Nov. 04, 2023. [Online]. Available: https://www.opengroup.org/togaf

[118] "Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity." Accessed: Nov. 04, 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity

[119] "IT Spending and Staffing Benchmarks - Computer Economics by Avasant." Accessed: Nov. 04, 2023. [Online]. Available: https://www.computereconomics.com/it-spending-and-staffing-benchmarks/

[120] "March 3 2015 B - Mgt 45 March 3 2015 Relevant | Course Hero." Accessed: Nov. 04, 2023. [Online]. Available: https://www.coursehero.com/file/11200869/March-3-2015-B/

[121] "Bitcoin Wallets Comparison - Rank bitcoin, ethereum and multi crypto app's by features and

ir1061.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

platforms and compare BTC debit cards & prepaid cards | CryptoCompare.com." Accessed: Nov. 04, 2023. [Online]. Available: https://www.cryptocompare.com/wallets/#/overview

[122] "2024 Tech Trends: The State of IT Report." Accessed: Nov. 04, 2023. [Online]. Available: https://www.spiceworks.com/research/state-of-it/

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.
hide01.ir

INDEX

A

Access Control · 82, 172, 173, 175
Agile Methodology · 204
Annualized Loss Expectancy · 37
Application Hardening · 204
Architectural Views · 242
Auditing · 107, 108, 168, 172
Authentication · 168, 169
Authorization · 168
Autonomous SOC · 225

B

Balance Sheets · 234
Balanced Scorecard · 244
Blockchain · 208

C

Cash Flow Statements · 234
CIA Triad · 74
Cloud Security Alliance (CSA) · 79, 272
COBIT · 50, 103, 108
compensating controls · 36
Compensating Controls · 78
Compliance · 8, 1, 2, 66, 104, 109
Contingency Funding · 258
Control Catalog · 78
Control Lifecycle Management · 73
COSO · 51
COSO PDC · 75
Cost-Benefit Analysis (CBA) · 268
Culture of Security · 240

D

Database Hardening · 207
Database Security · 206
Decryption · 208
Defense-in-Depth Model · 75
DevSecOps · 201
Digital Forensics Life Cycle · 145
Digital Signatures · 208
Disaster Recovery Planning (DRP) · 139

E

EC-Council Code of Ethics · 18
Encryption · 82, 208, 210, 211, 212, 213
Enterprise Architecture (EA) · 247
Ethics · 17
Event Management · 149, 150

F

Factor Analysis of Information Risk · 52
FAIR · 52
Federal Enterprise Architecture Framework (FEAF) · 252
Financial Metrics · 257

G

Governance · 8, 1, 2, 3, 69, 108, 132

H

Hashing · 210
HITRUST · 68, 272
Hybrid Assessments · 57

I

Incident Response · 142, 143, 144, 153, 155
Income Statements · 234
Information Security Management System (ISMS) · 70
Information Sharing and Analysis Centers (ISAC) · 158
Information Technology Infrastructure Library (ITIL) · 51
Inherent Risk · 26
Internet of Things Security (IoT) · 198
ISO 27001 · 272
ISO 27005 · 61
ISO/IEC 27001:2013 · 89
ISO/IEC 27002:2013 · 89
ISO/IEC 27003:2017 · 90
ISO/IEC 27004:2016 · 90
ISO/IEC 27005:2018 · 21
ISO/IEC 27014:2013 · 90
ISO/IEC 27017:2015 · 90
ISO/IEC 27018:2014 · 91
ISO/IEC 27032:2012 · 91
ISO/IEC 27034-1:2011 · 91
ISO/IEC 27035-1:2016 · 91
ISO/IEC 27036-1:2014 · 92
ISO/IEC 27037:2012 · 92
ISO/IEC 31000:2018 · 21
ISO/IEC TR (Technical Report) 27016:2014 · 90
ITIL · 70, 246

K

Key Controls · 78
Key Management · 209

M

Master Service Agreement (MSA) · 263
Maturity · 4, 80, 107
Mobile Device Security · 196, 198

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

N

Network Security · 182, 183, 189
NIST Cybersecurity Framework · 71
NIST Minimum Security Controls · 77
NIST risk assessment process · 49
NIST Risk Management Hierarchy · 48
NIST SP 800-30 · 20
NIST SP 800-37 · 20
NIST SP 800-39 · 21

O

OCTAVE · 52, 53
Organizational Structure · 6

P

P6 Model · 80
Patch Management · 205
PCI DSS · 83, 93
Penetration Testing · 160
PHYSICAL SECURITY · 177
PKI · 82, 209
Privacy · 2, 79, 85
Procurement Life cycle · 267

Q

Qualitative Assessments · 57
Quantitative Assessments · 57

R

Request for Information (RFI) · 263
Request for Proposal (RFP) · 262
Residual Risk · 26
Risk Acceptance · 35, 43
Risk Analysis · 41
Risk assessment · 40
Risk Assessment Process · 24
Risk Assessment Types · 24
Risk Calculation · 36
Risk Categories · 26
Risk Communication · 43
Risk Evaluation · 42
Risk Feedback · 43
Risk Identification · 41
Risk Management · 8, 1, 3, 265
Risk management frameworks · 37
Risk Management Frameworks · 38
Risk Management Lifecycle · 56
Risk Modification · 34
Risk Monitoring · 44
Risk ownership · 23
Risk Registry · 57
Risk Retention · 34
Risk Sharing · 35
Risk Transfer · 35
Risk Treatment · 33, 42
Risk Treatment Options · 33

S

Secure SDLC · 200
Security Awareness · 195
Security Budget · 254, 259, 261
Security Controls · 8, 66, 72, 77, 81, 189, 198, 216, 222
Security Drivers · 5
Security Information and Event Management (SIEM) · 149
Security Policy · 9, 10, 11
Security Program Funding · 254
Security Strategic Plan · 235
Service Level Agreement (SLA) · 263
Sherwood Applied Business Security Architecture (SABSA) · 251
Software-Defined Cybersecurity · 226
Standard Contract Language · 266
Statement of Objectives (SOO) · 262
Statement of Work (SOW) · 262
subjective risk assessments · 24

T

TARA · 53, 54
Technology Refresh · 257
Terms and Conditions (T&C) · 263
The Open Group Architecture Framework (TOGAF) · 249
Third-Party Attestation Services (TPRM) · 271
Threat Hunting · 163
threat hunting loop · 164
Threat Intelligence · 157
Threats · 194
Total Cost of Ownership (TCO) · 262

U

User Access Behavior Management · 173

V

VENDOR MANAGEMENT · 266
Virtualization · 214
Virtualization Risks · 215
Virtualization Security · 216, 217
Voice over IP Security · 193
Vulnerabilities · 195
Vulnerability Management · 158, 160

W

Waterfall Methodology · 203
Wireless Risks · 192

Z

Zachman Framework · 248

hide01.ir

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.