System Security Certified Practitioner - SSCP®

Certification Course Overview

Kevin Henry CISA, CISSP-ISSMP, SSCP
Pluralsight Author

kevin@kmhenrymanagement.com

Systems Security Certified Practitioner - SSCP®

Earning a globally recognized IT security administration and operations certification like the SSCP is a great way to grow your career and better secure your organization’s critical assets.

What Is the SSCP®?

SSCP certification demonstrates you have the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures established by the cybersecurity experts at ISC2.

Prove your skills, advance your career, and gain the support of a community of cybersecurity leaders here to help you throughout your career.

https://www.isc2.org/certifications/sscp

SSCP® Examination Modules

SSCP Domain	Exam Weighting
Security Concepts and Principles	16%
Access Controls	15%
Risk Identification, Monitoring, and Analysis	15%
Incident Response and Recovery	14%
Cryptography	9%
Network and Communications Security	16%
Systems and Applications Security	15%

Preparing for the SSCP® Examination

Exam Review Tips

Study Guide

Sample Questions

The SSCP® Examination

150 items

Passing score of 700 points of a possible 1000

Security Concepts and Practices for SSCP®

Security Concepts and Controls

Kevin Henry CISA, CISSP-ISSMP, SSCP
Pluralsight Author

kevin@kmhenrymanagement.com

Course Introduction

This domain of the SSCP® is divided into three sections:

- Security Concepts and Controls
- Asset Management and Security
- Personnel Security

This domain is weighted for 16% of the SSCP examination

Key Points

The security practitioner is an important member of the information security team

- Must understand the relationship between business and security
- Ensure that security practices are being followed

Security and the Business

The Purpose of Business

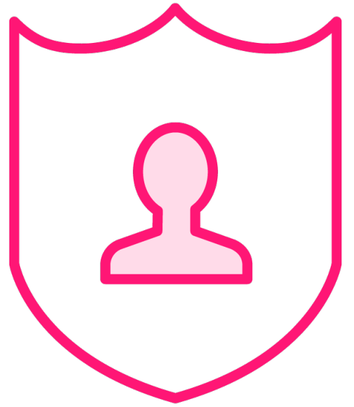
Provide products and services

- Military
- Law enforcement
- Commercial
- Not-for-profit
- Government

The Role of Information Security

Support business operations

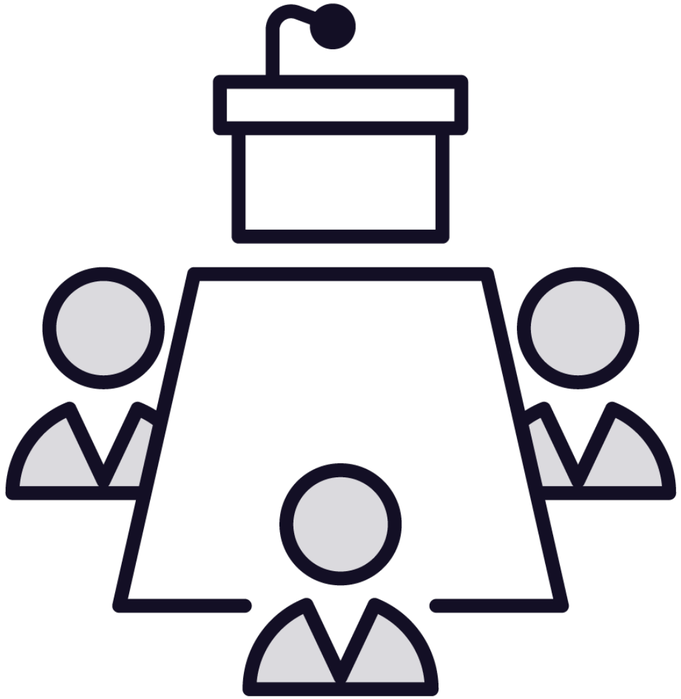
Reach business goals
and objectives



Not to aim for the ultimate security level

The CIA Triad

What Is Information Security?



Perception

- Security professionals
- Managers
- Users
- Regulatory bodies
- Customers
- Auditors

How Much Security Is Needed?

Adequate

Regulations and laws

Customer expectations

Shareholders

Business partners

Confidentiality

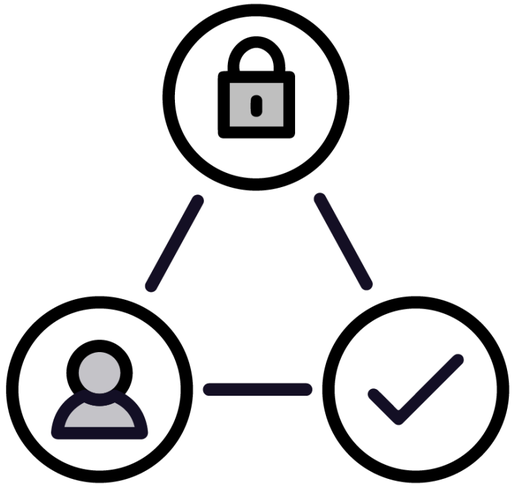
Privacy

- GDPR

Secrecy

Protection from unauthorized disclosure

Integrity

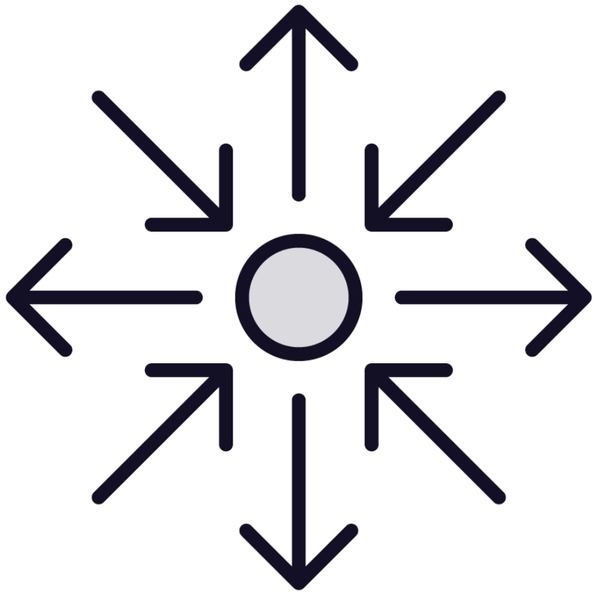


Protection of information and information process flows from improper or unauthorized modifications

Accuracy

Precision

Availability



Ensure that data and information systems are accessible when required

- Networks
- Applications
- Equipment

Protection from destruction

Sensitivity and Criticality

The enforcement of the CIA triad is based on the requirements to protect sensitivity and criticality

- Sensitivity
  - The degree to which an entity (an organization or person) could be harmed by a loss of confidentiality or integrity
- Criticality
  - The degree to which an entity could be harmed by the loss of availability

Key Points Review

The CIA triad was developed to describe security concepts to non-security personnel

All three legs of the triad are important

- Depending on the type of organization

Enforcement of CIA

Reasons for Confidentiality

Laws and regulations

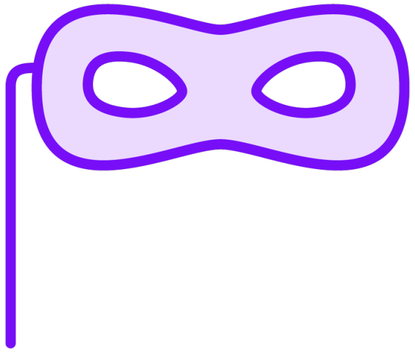
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)

Competitive Advantage

- Research
- Trade secrets
- Contractual agreements
  - Non-disclosure agreements (NDAs)
  - Customer expectations

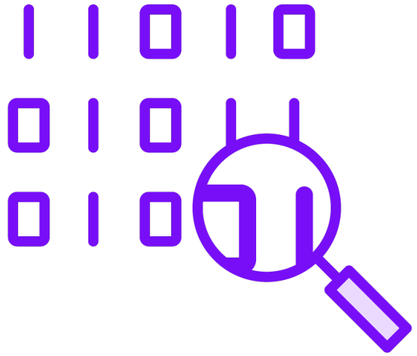
Enforcing Confidentiality

Access Controls
Encryption
Need-to-know
Least privilege



Masking

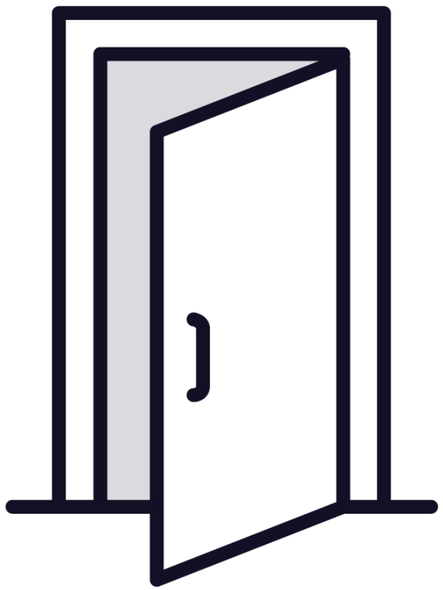
Obfuscation



Bit-splitting

Enforcing Availability

Reasons for Availability



Ensure information and systems are accessible when required

- Support business operations
  - Health and safety
  - Industrial operations
    - ICS and SCADA
- Meet contractual requirements
- Ensure customer trust

Enforcing Availability

Backups

Full, incremental, differential

Journals

RAID

Transactions, applications, operating systems, configurations, utilities

Enforcing Availability

Clusters

Replication

- Equipment
- Networks
- Personnel
- Facilities
- Supply chain
  - Continuity plans of Cloud Service Providers

Business Continuity

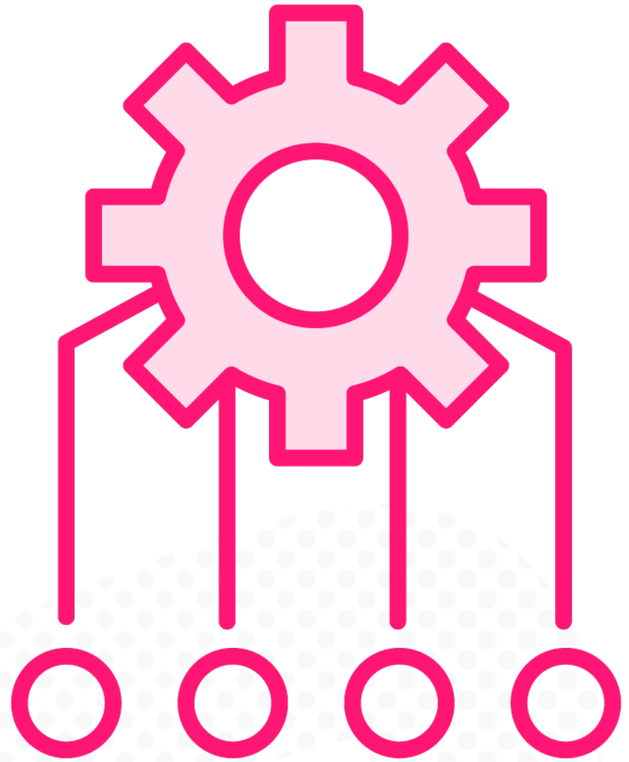
Ensuring continuity of delivery of products and services

Critical business functions

Recovery Time Objective

Recovery Point Objective

Disaster Recovery Planning



Key Points Review

Confidentiality and Availability may seem to be opposites – how can you make information available without breaching confidentiality

Both are important parts of securely supporting business operations

Ensuring Integrity

Reasons for Integrity

Regulations

Financial transactions and reporting (ATM)

Healthcare (Pharmaceuticals)

Trust

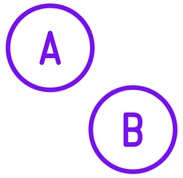
Customer orders

Accountability

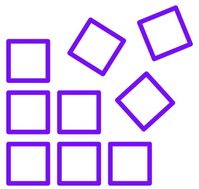
Enforcing Integrity

- Checksums
- Check digits
- Parity bits
- Message Authentication Codes (MAC)
- Hash or Digest algorithms
- Header and Trailer records
- Encryption

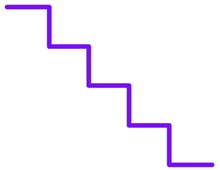
Separation of Duties



Also known as Segregation of Duties (SoD)

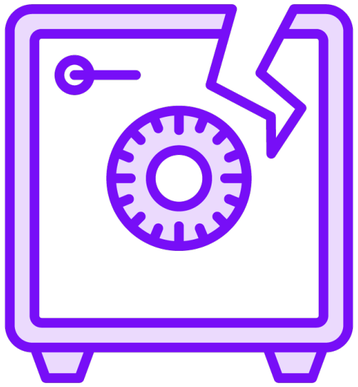


Dividing a process into multiple parts where each part is performed by a different entity (person or process)

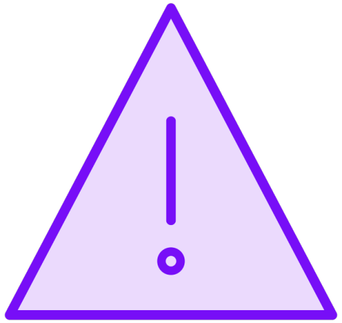


No one person controls an entire transaction from its inception through to its completion

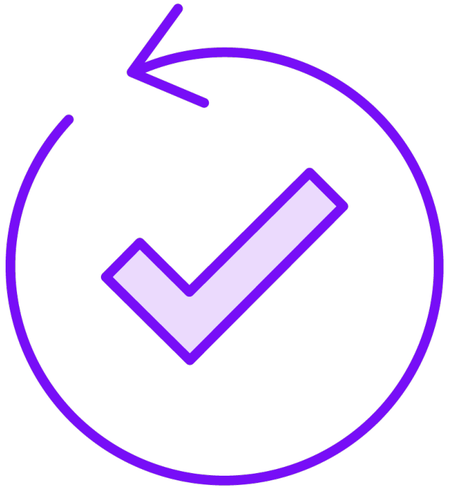
Reason for Separation of Duties



Fraud

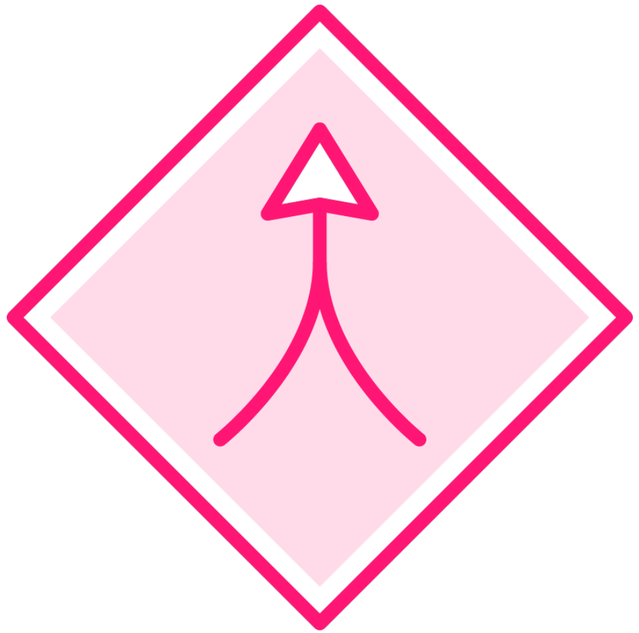


Mistakes
Errors
Omissions



Cross-training
Single point of failure (personnel)

Challenges with Separation of Duties



Collusion

Lack of review

Loss of efficiency

- Delay in processing
- Frustration - ability to learn new skills

May be impractical in small organizations or departments

- Often lost during a crisis or emergency

Non-repudiation

Repudiate:

Refuse to accept or be associated with

Deny the truth or validity of

Refuse to fulfill or discharge (an agreement, obligation, or debt)

Non-repudiation:

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither party can later deny having processed the information

Oxford Languages and https://csrc.nist.gov/glossary/term/non_repudiation

Enforcing Non-repudiation

Digital signatures

Public Key Infrastructure (PKI)
Certificates

Trusted Third Parties (TTP)

Key Points Review

Integrity is a wide-ranging topic including the concepts of authorization, separation of duties and non-repudiation

Quick Summary

There are key points to remember as you review this module:

- Security must have a business orientation
- Security is much more than secrecy or privacy
- Security is a key part of all business operations – even business continuity and supply chain

Security Controls

Controls

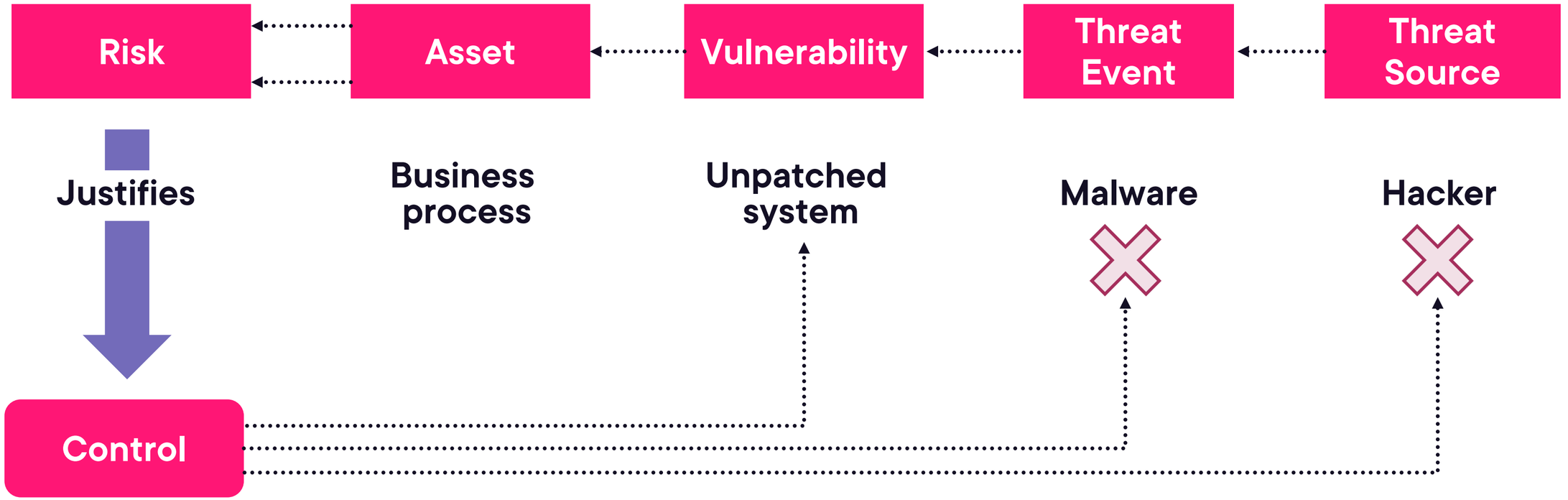
Controls are used to address risk

The identification of risk justifies the implementation of controls to mitigate the risk

BUT

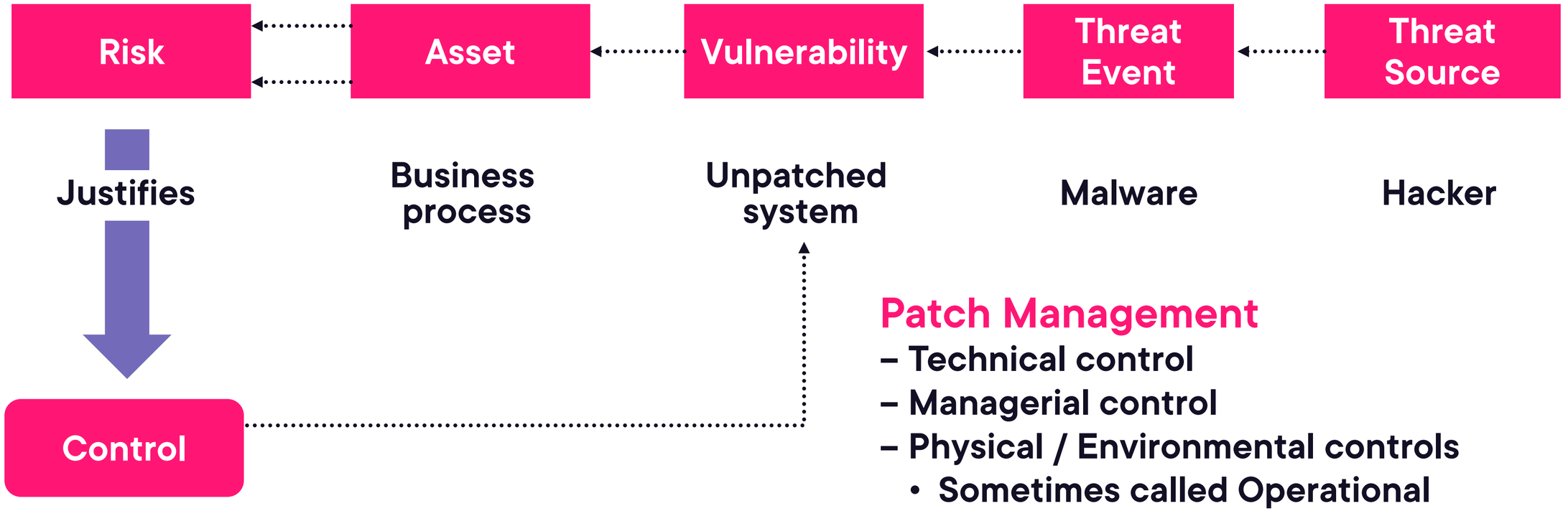
The assessment of controls should clearly indicate their effectiveness in mitigating the identified risk

Risk and Controls



Covered in more detail in Risk Identification, Monitoring, and Analysis course

Risk and Controls



Patch Management

- Technical control
- Managerial control
- Physical / Environmental controls
  - Sometimes called Operational

Covered in more detail in Risk Identification, Monitoring, and Analysis course

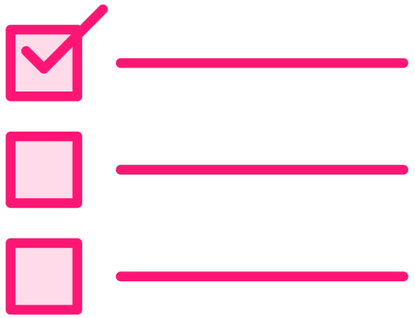
Key Points Review

Controls are used to address risk

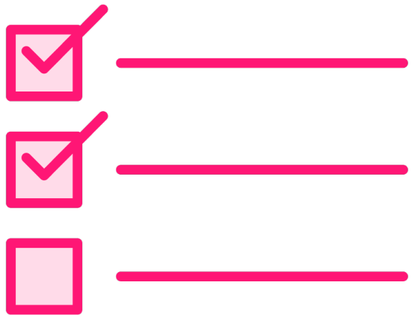
A control may be managerial, technical, or physical — but often requires a combination of controls working together — what good is a firewall without a policy?

Types of Controls

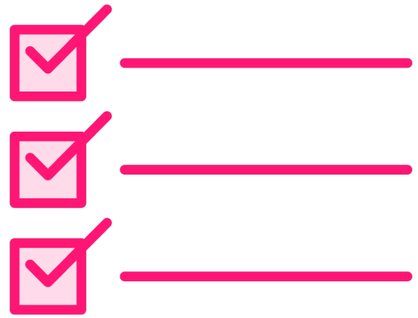
Types of Controls



Managerial / Administrative

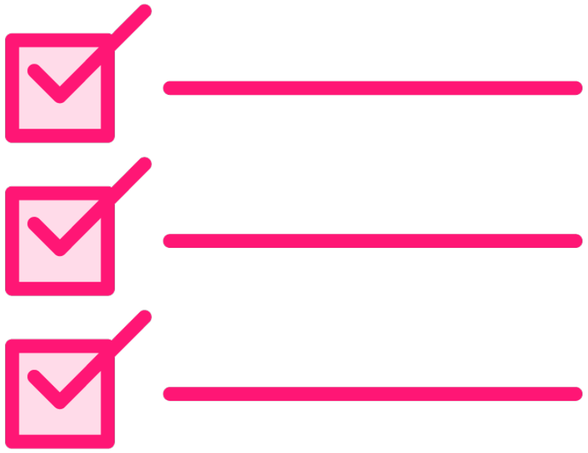


Technical/ Logical



Physical / Environmental

Administrative Controls



Policies

Procedures

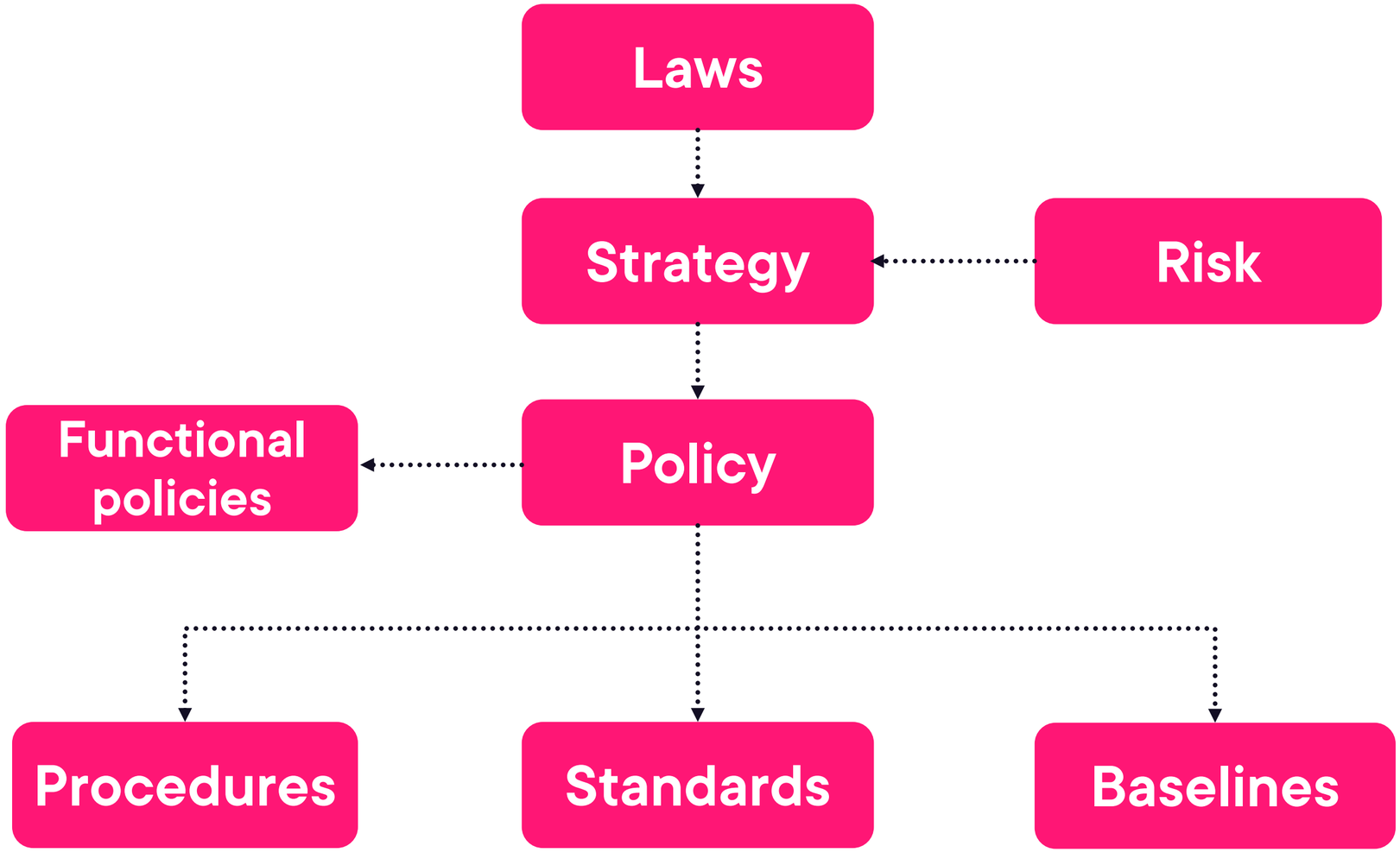
Standards

Baselines

Asset management

- Information classification

Policy Hierarchy



Policies

Endorsed by management

Reflect management's commitment/intention

Aligned with organizational culture

Non-technical

Up-to-date/ownership

Communicated

Exceptions

Functional Policies

Technical

Single topic?
e.g., Wireless connectivity, BYOD

Changed as required

Easier to modify

Procedures

Step-by-step actions

- ‘how-to’

Consistency

Standards

INTERNATIONAL STANDARD

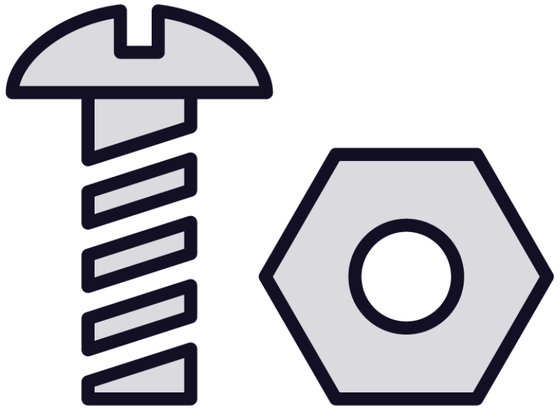
ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

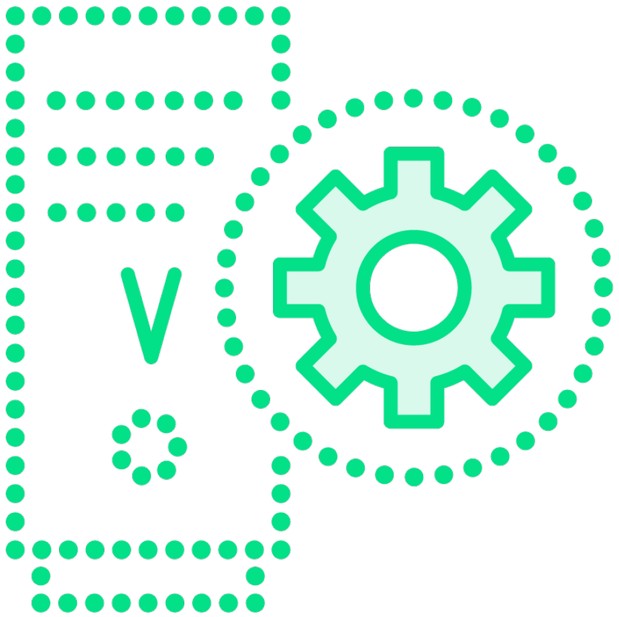
Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

May be based on a standards document
ISO/IEC 27001



May be standard for equipment
Hardware
Software

Baselines



Configuration

- Mandated configuration
  - Password length
  - Hardware or software configuration
    - Desktop
    - Operating system hardening
    - Virtual machine

Key Points Review

Administrative controls set out policies, procedures, standards and baselines

It is easy for technically-minded experts to overlook the value of, and need for, administrative controls

Technical or Logical Controls

Technical Controls

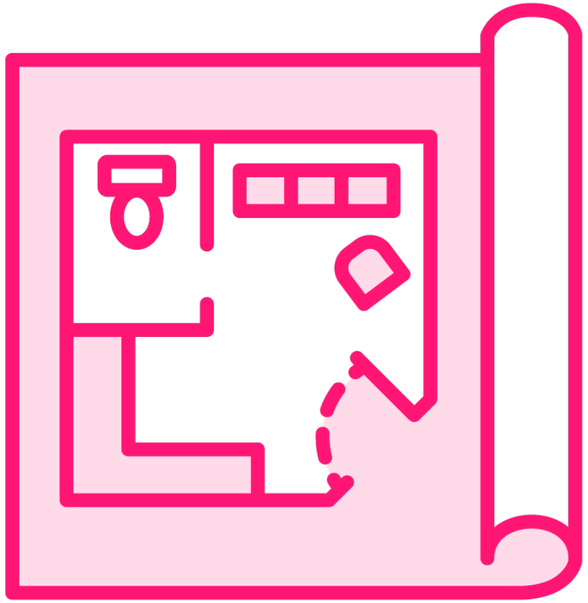
Hardware

- Standalone security devices (e.g., SIEM)
- Security features in a device
  - Firewalls
  - IDS/IPS

Software

- Access Control Lists (ACLs)
- Logging

Deployment of Technology



Architecture

- Placement

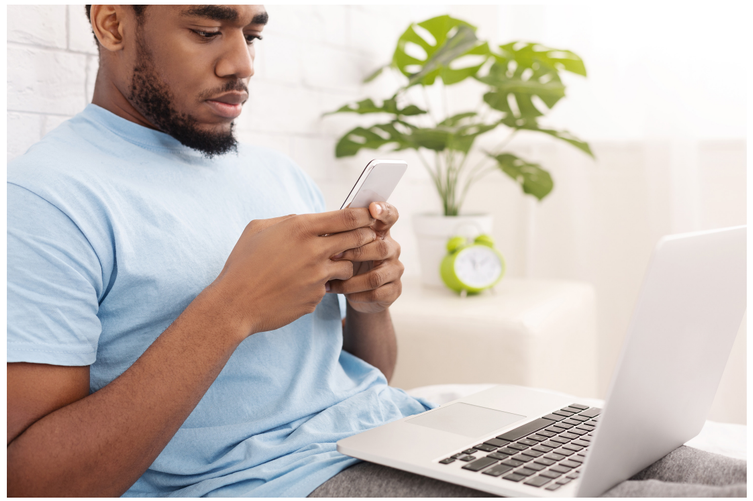
Configuration

Patching

Maintenance

Monitoring

Examples of Technical Controls



Session management

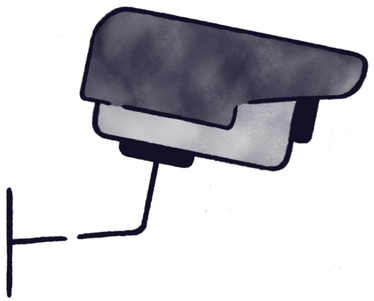
- Multi-factor authentication
- Timeouts

Passwords:

- Password creation
- Password storage
- Password expiry

Physical Controls

Physical Controls



The most obvious controls!

- Fences and bollards
- Security guards
- Cameras
- Locks
- Motion sensors
- Mantraps and turnstiles

Other Physical Controls

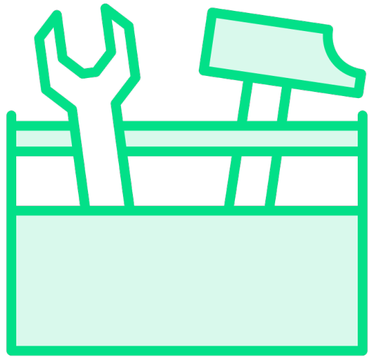
Power

Fire

Water

Heating, ventilation, and air conditioning (HVAC)

Physical Control Maintenance



Repairs and maintenance

Monitoring

Response

Key Points Review

There really is NO security without physical security

Technical security controls require maintenance, and administrative and physical support

Bringing It All Together

Types of Controls

Directive

Deterrent

Preventive

Corrective

Detective

Recovery

Examples of Controls

Controls	Administrative	Technical	Physical
Directive	Policy	Privacy notice	Do Not Enter sign
Deterrent	Disciplinary action	Notice of monitoring	Beware of Dog sign
Preventive	Separation of Duties	Password	Fence
Detective	Audit	IDS	Smoke detector
Corrective	Suspension	Isolation	Fire extinguisher
Recovery	Awareness	Restore from backups	Rebuild

Safeguards
Proactive
Controls

Countermeasures
Reactive Controls

Compensating Controls

A control that addresses a weakness or lack in other controls

The guard by a turnstile

The ability to reset a password

Multi-purpose Controls

Closed Circuit Television (CCTV)

- Acts as a:
  - Deterrent
  - Detective
  - Corrective

Layered Defense

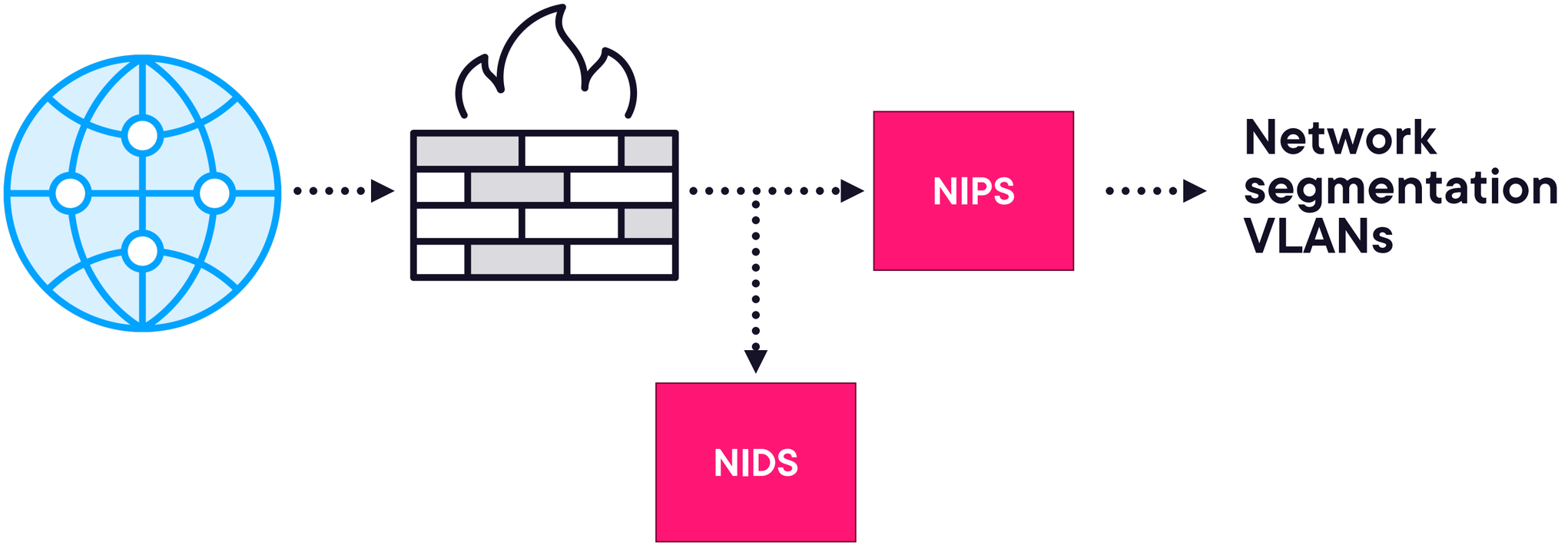
Layered Defense

Defense in depth

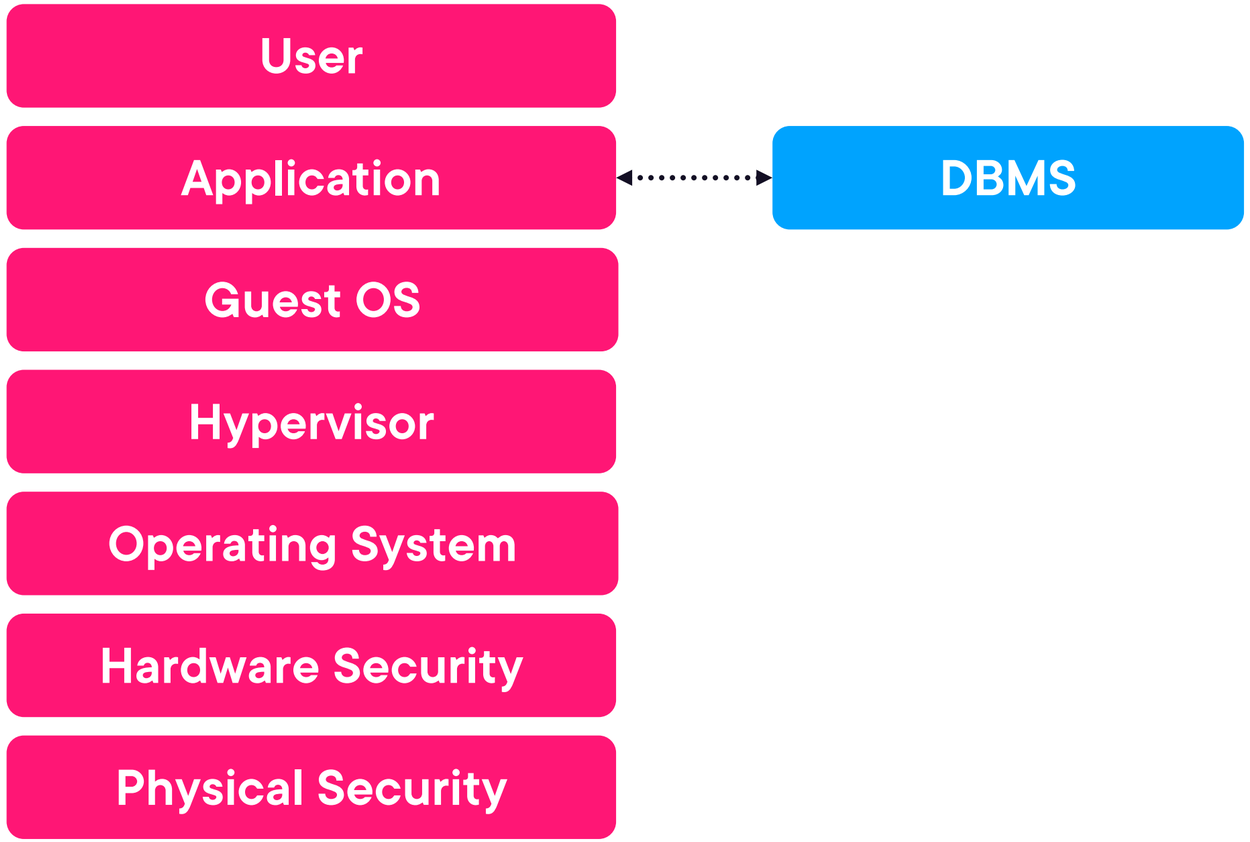
Avoidance of single point of failure

A type of compensating control

Layered Network Defense



Vertical Defense in Depth



Key Points Review

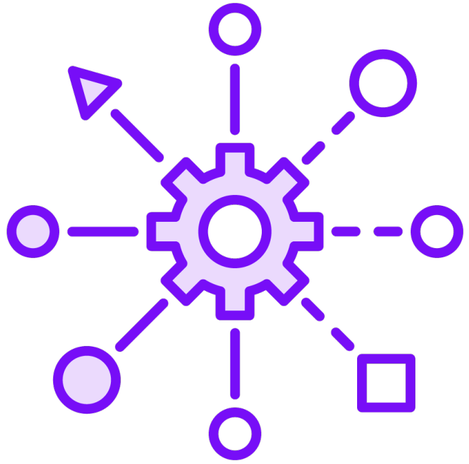
Security should be built into business processes

Single points of failure should be identified and mitigated

The Impact of Controls

Disadvantages of Controls

Performance



Productivity

Frustration

Defeating Controls

Bypassing controls

Disabling controls

- Logs
- Alarms

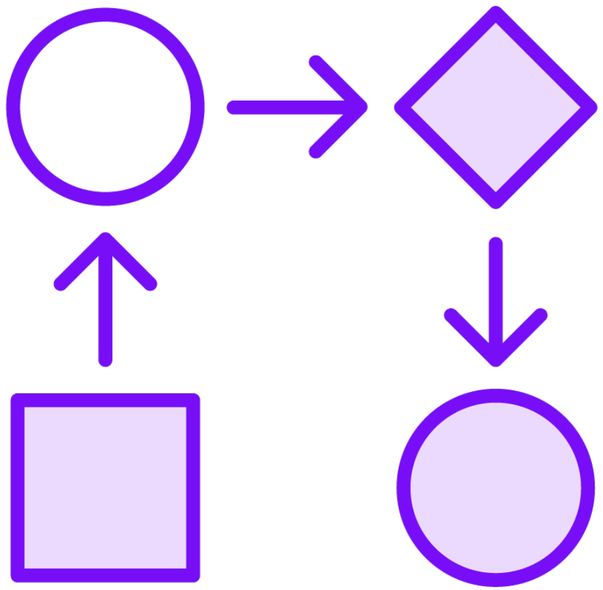
Lack of monitoring

Lack of response

Control Risk

The risk that a control will not effectively mitigate a risk

Monitoring



Ownership of control

Policy

- Compliance with laws and policy
  - Access controls

Procedures

- Periodic review

Reporting

Verification and Validation

Verification

The control was implemented as designed
The control is operating as intended

Validation

The control is the ‘right’ control

Monitoring Skills

Filtering

- Tools
- Scripts
- Experience
- Record of previous incidents

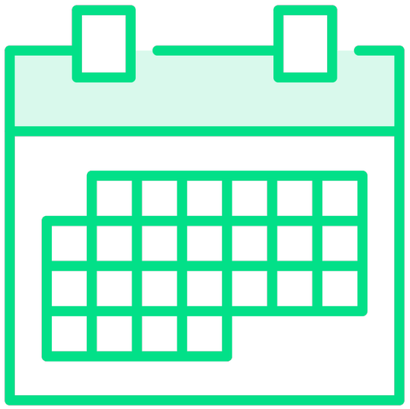
Metrics

Key Performance Indicators

Consistent

Key Risk Indicators

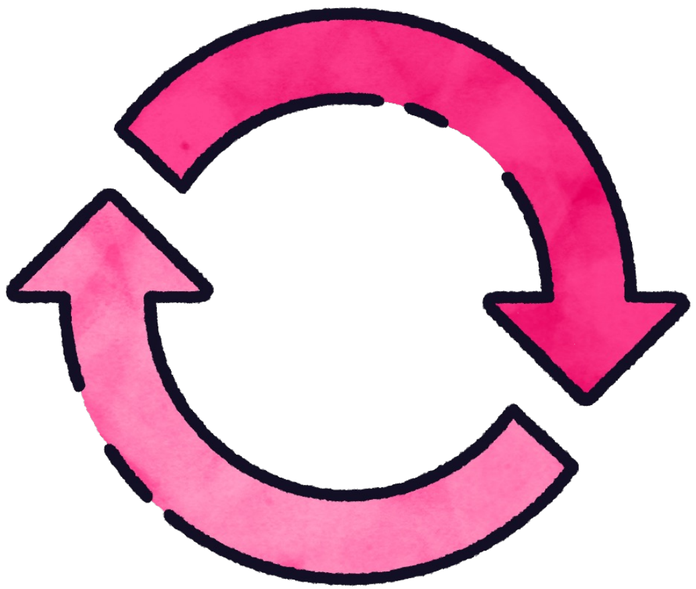
Reporting Frequency



Scheduled

Ad-hoc

Reporting Format



Consistency in format

Cyclical: daily, monthly, annually

- Exceptions or aberrations

Key Points Review

Controls are the center-piece of security

Controls are used to mitigate risk and protect assets

Controls must be designed, implemented, configured, maintained, and monitored for effectiveness