Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 01: Security and Risk Management

Learning Objectives

By the end of this lesson, you will be able to:

- Analyze information security management for safeguarding organizational assets
- Implement the process of security policy development to ensure compliance with security standards
- Evaluate information risk management strategies for minimizing potential security threats
- Manage personnel security and security function processes for protecting sensitive information
- Analyze instances of computer crime to develop preventive measures
- Develop a business continuity plan (BCP) for ensuring operational resilience during disruptions

Overview of Information Security

What Is Information Security (InfoSec)?

It is the practice of protecting information by mitigating information risks.

It is about safeguarding data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information can be anything valuable, including customer data, financial records, intellectual property, personal details, and even classified government information.

Why Information Security?

- Digital transformation increases cyber threats, making information security essential to protect sensitive data.
- Information security safeguards both business operations and personal safety, extending beyond traditional IT concerns.
- Security breaches can lead to severe consequences, including identity theft and financial fraud, causing extensive damage.
- Artificial intelligence and deepfakes amplify risks, making robust information security more critical than ever.

Factors Impacting Information Security

Nature of business

Security culture

Legal and regulatory compliance

Management support

Risk appetite

Industry threats

Information Security Management

It describes the controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

It ensures the implementation of the following:

- Information security policies
- Standards
- Procedures
- Guidelines
- Baselines
- Information classification
- Risk management
- Security organization
- Security education

Information Security Governance

It is a systematic approach used by organizations to manage and protect their information assets, ensuring confidentiality, integrity, and availability of data.

It is a structured approach for managing and protecting sensitive data.

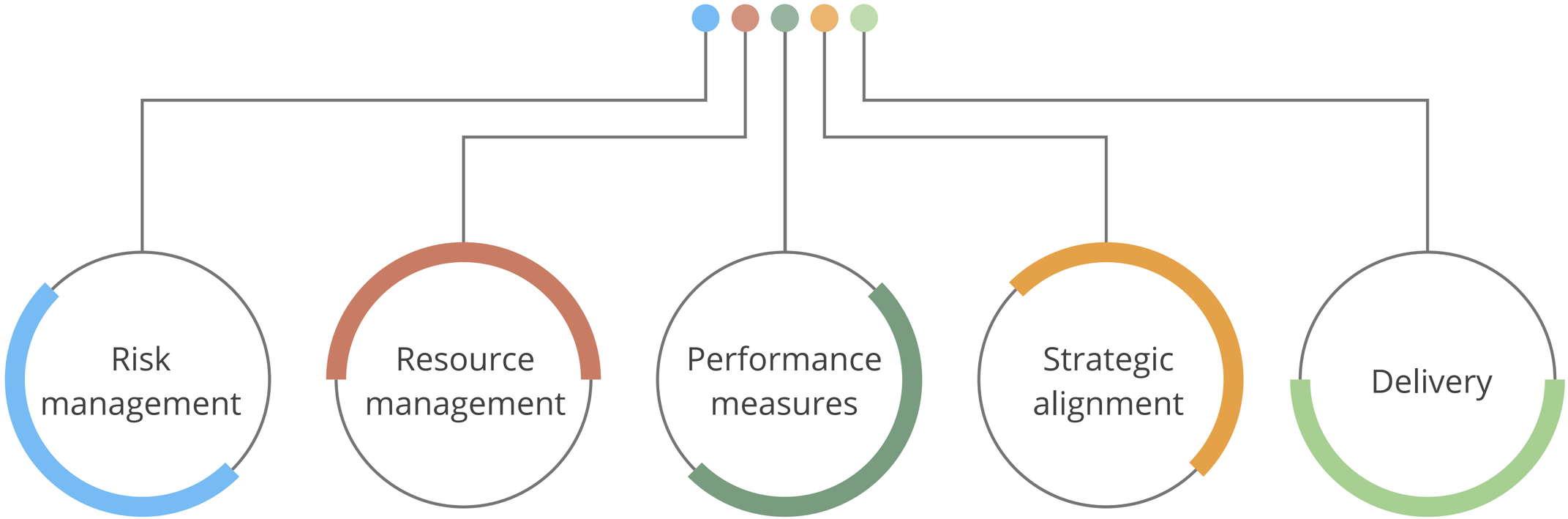
It aligns information security objectives with business goals.

It implements controls and measures for safeguarding information assets.

It provides systematic management and protection of information.

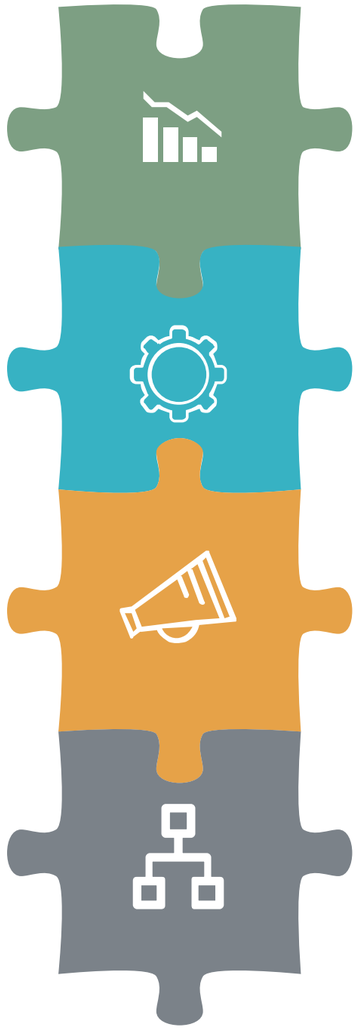
Information Security Governance: Principles

The major focus of governance is on:



Information Security Governance: Goals

It is intended to guarantee:



- Risks are reduced.
- Security activities are verified with appropriate information.
- Information security investments are appropriately directed.
- Executive management can determine program effectiveness.

Governance, Risk Management, and Compliance (GRC)

It is a comprehensive framework that helps organizations manage their overall risk exposure and ensure compliance with relevant laws, regulations, and industry standards.

This framework helps organizations:

- Identify, assess, and mitigate risks to protect the organization
- Adhere to relevant laws, regulations, and industry standards, ensuring compliance
- Implement effective governance processes and structures

Governance, Risk Management, and Compliance (GRC)

The following characteristics of GRC must be considered during its implementation:

- It is different for every organization and varies based on the type of organization.
- It depends on an organization’s mission (business), size, industry, culture, and legal regulations.
- Its ultimate responsibility is to protect the organization’s assets and operations, including their IT infrastructure and information.

GRC: Governance

It is the responsibility of the board of directors and senior management of the organization.

GRC: Governance

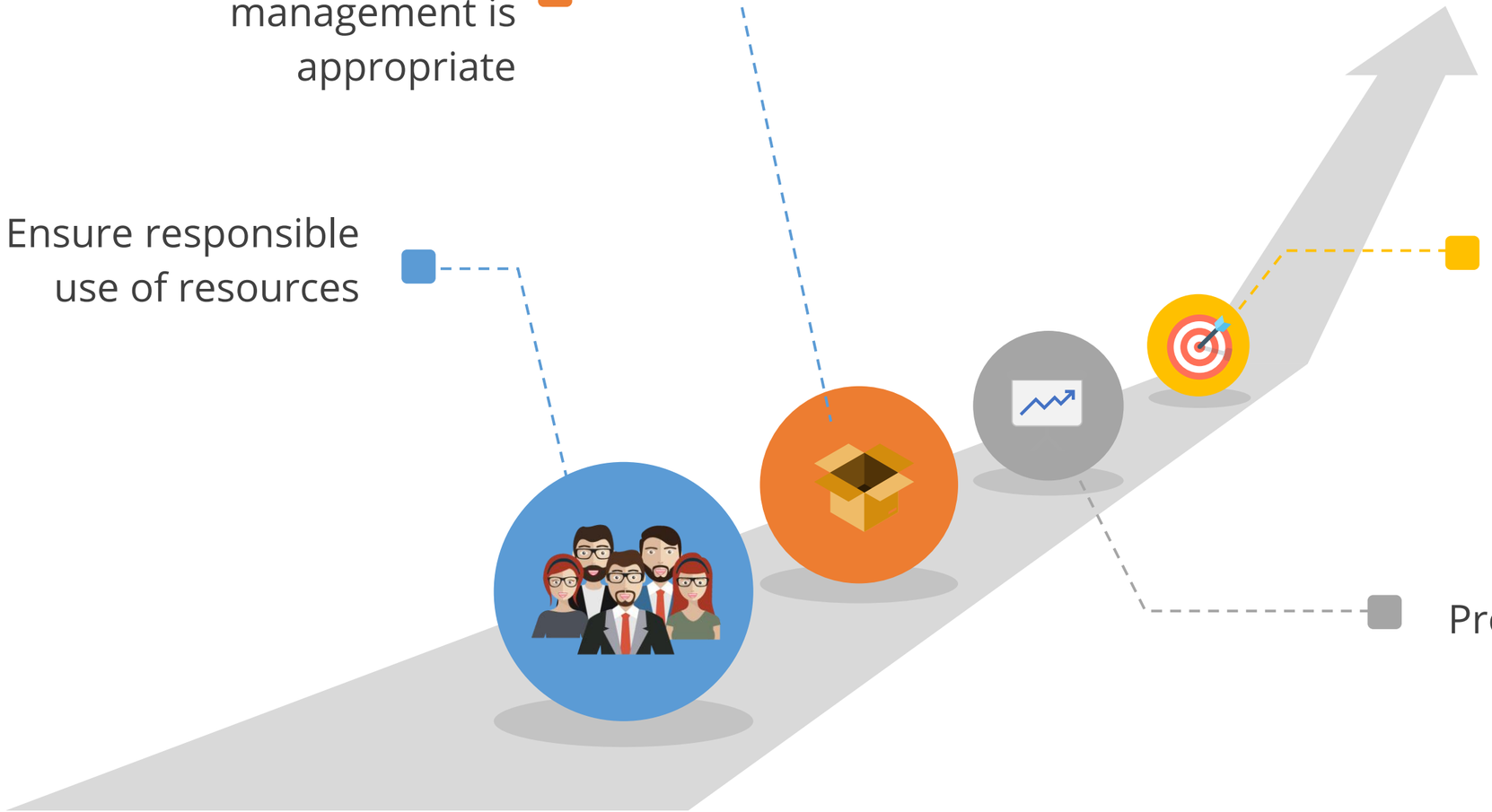
The goals of governance include:

Ascertain if risk management is appropriate

Ensure responsible use of resources

Ensure that objectives are achieved

Provide strategic direction



Managing Outsourcing Governance

Outsourcing is the subcontracting of a business process to a third-party company.

Risks associated with outsourcing

- Loss of control of confidential information
- Accountability
- Compliance

Secure outsourcing

- On-site assessment
- Document exchange and review
- Policy and process review

GRC: Risk Management

It is the process by which an organization manages risk to acceptable levels. It requires the development and implementation of internal controls to manage and mitigate risk throughout the organization, including:

Financial and investment risk

Physical risk

Cyber risk

GRC: Compliance

It is the act of adhering or the ability to demonstrate adherence to mandated requirements defined by laws and regulations.

It also includes voluntary requirements resulting from contractual obligations and internal policies.

Overview of Cybersecurity

Cybersecurity

It is the process of securing sensitive data and critical systems from cyber threats.

It safeguards enterprises from intentional attacks, data breaches, and security incidents, and their consequences.

It protects information assets by addressing threats to data that is processed, stored, or transmitted across interconnected systems.

Goal of Cybersecurity

The primary objective of cybersecurity is to preserve the confidentiality, integrity, and availability of an organization's critical assets from attack, damage, or unauthorized access.

Why Is Cybersecurity Important?

It is important for the following reasons:

Increase in cybercrime due to technological advancement

Shift to online business, demanding protection of generated personal, financial, and operational data

Presence of crime syndicates, cyber armies, and financial frauds

Difference Between Information Security and Cybersecurity

Feature	Information security	Cybersecurity
Scope	Protects all types of information (physical and digital)	Focuses on protecting digital assets and networks
Focus area	Ensures confidentiality, integrity, and availability	Defends against cyber threats like hacking and malware
Coverage	Broad, covering physical and digital information	Narrow, targeting digital data and systems
Primary concerns	Preventing unauthorized access to information	Securing systems and data from online threats
Examples	Safeguarding documents and controlling database access	Defending against phishing and securing cloud systems

Impact of Risks of Security on Business

Reputational and financial loss

Business interruption loss

Loss of customer confidence

Legal action against company

Intellectual property loss

Data breach

Terrifying Cybercrime Statistics

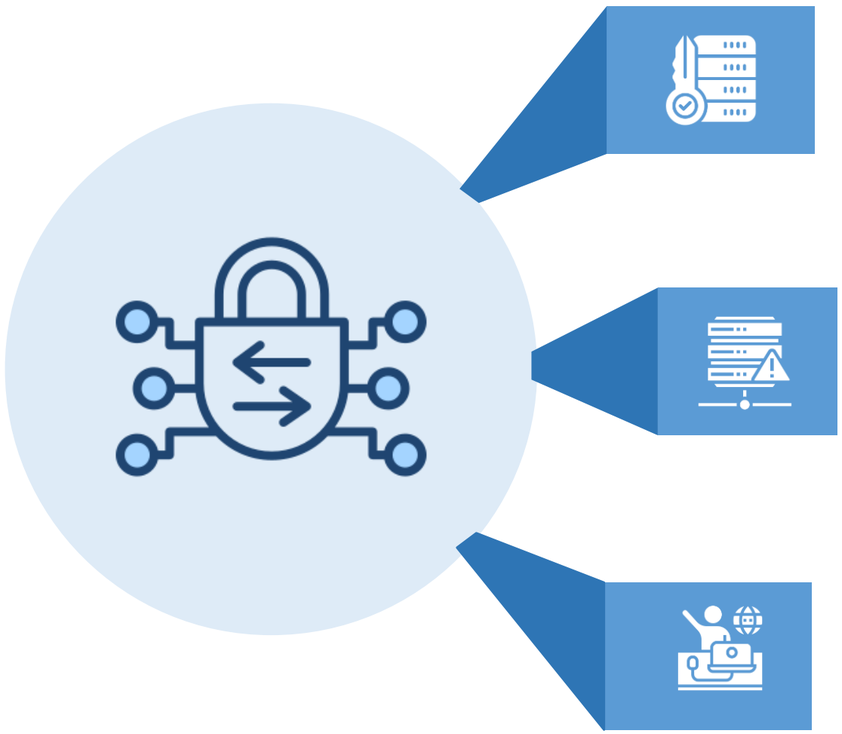
The following are some recent trends that make cybersecurity more important:

- In 2023, five billion data breaches compromised approximately 867 million records.
- Over 2.8 million malicious apps were blocked from entering the Google Play Store during the same year.
- Ransomware attacks on the healthcare industry are expected to increase fourfold soon.
- Cybercrime costs are expected to reach $23.84 trillion by 2025.
- The number of passwords worldwide is expected to reach 350 billion by 2025.
- More than 60% of fraud is projected to originate from mobile devices.
- Personal data is sold for as little as $0.20.
- Encryption is used by 90% of hackers.

Approaches to Cybersecurity

Organizations adopt different approaches to cybersecurity based on their regulatory requirements, specific risks, or lack of structured strategies.

These approaches guide how security measures are implemented to safeguard digital assets:



Compliance-based: Relies on regulations or standards to determine security implementation

Risk-based: Relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk

Ad hoc: Implements security with no rationale or criteria

Overview of (ISC)^2 Professional Ethics

(ISC)² Professional Ethics

The International Information Systems Security Certification Consortium (ISC)² has established a **Code of Ethics** outlining the ethical responsibilities of its certified members.

It serves as a guideline for professional conduct in information security.

It is critical for maintaining integrity and professionalism in information security.

Every certified professional is expected to adhere to these principles.

(ISC)² Professional Ethics: Categories

It has the following two categories:

Code of Ethics Preamble

- The safety and welfare of society require adherence to the highest ethical standards.
- One's duty to principles and others also demands visible adherence to these standards.
- Strict adherence to this code is a condition of certification.

Code of Ethics Canons

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principles
- Advance and protect the profession

Code of Ethics

Ethics are the principles and values used by an individual to govern their actions and decisions.

A **code of ethics** provides a general understanding of the ethical or moral responsibilities that the governing body, employees, and volunteers are expected to meet while working for the organization.

An **organizational code of ethics** expresses the overarching principles or ideals that guide an organization’s decisions and actions when conducting operations and service delivery.

Organizational Code of Ethics

A code of ethics can help the organization to:

Show customers that it values integrity

Define the terms of ethical standard of behavior at work

Guide decision-making in difficult situations

Quick Check

You are working as a CISSP-certified cybersecurity professional at a nonprofit organization. Which of the following ethical obligations are you required to follow?

A. $(ISC)^2$ code of ethics

B. Organizational code of ethics

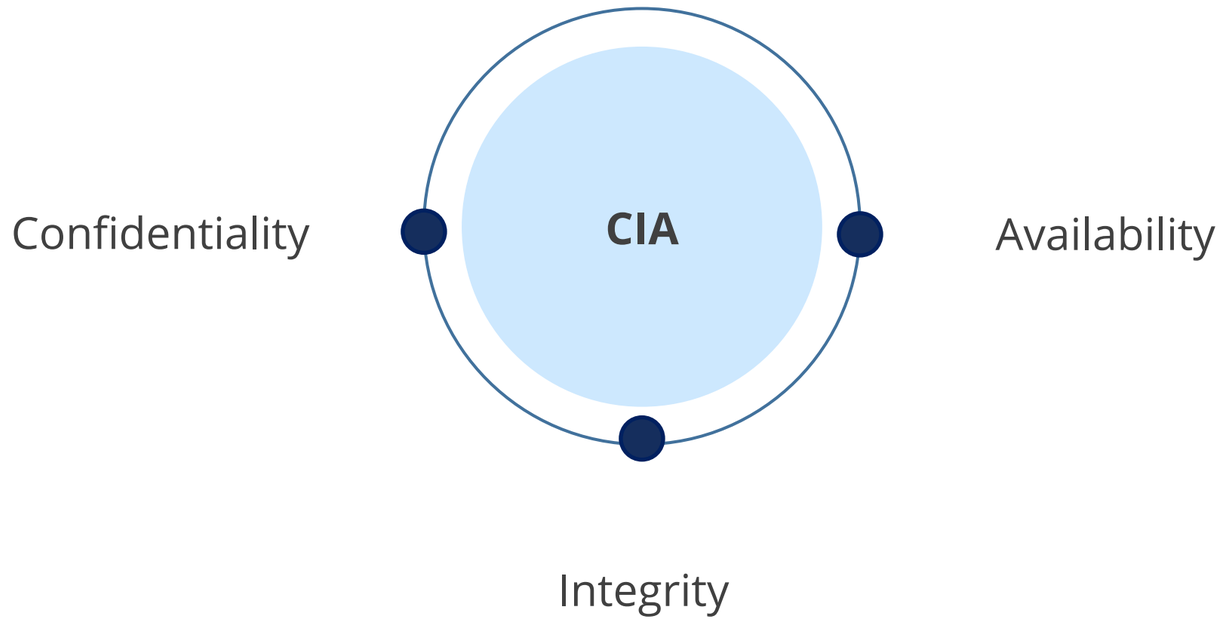
C. Federal code of ethics

D. RFC 1087

Securing Information with the CIA Triad

CIA Triad

CIA stands for confidentiality, integrity, and availability, which are the primary goals of cybersecurity.



CIA Triad: Confidentiality

Confidentiality

Confidentiality means that private or confidential information should not be disclosed to unauthorized individuals.

CIA Triad: Confidentiality

Intentional attacks

Man-in-the-middle attack, packet sniffing, and hacking

Accidental leakage

Untrained employees

Authentication and authorization failures

Access to a least-privileged entity

Hardware or software failures

Improper media sanitization

CIA Triad: Confidentiality

The following are some countermeasures to ensure confidentiality:

Encryption

Converts information to an unreadable format

Access control

Prevents users from accessing confidential information without permission

Administrative policies

Implements confidentiality policy and non-disclosure agreement (NDA) as deterrent controls

CIA Triad: Integrity

Integrity

Integrity means that information or systems should be protected from intentional, unauthorized, or accidental changes.

CIA Triad: Integrity

The following are the various threats to integrity:

Intentional alteration
(Virus attack and database hack)

Environmental factors
(Electromagnetic interference)

System malfunction
(Improper software configuration)

Accidental modifications
(Lack of input validation and training)

CIA Triad: Integrity

The following are some countermeasures to ensure integrity:

Cryptographic hash

Hash value of a file can be used to figure out if the file has been modified.

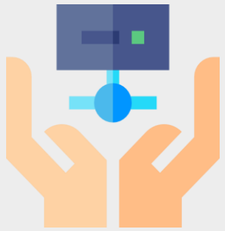
Checksums

It can detect errors and reconstruct missing data.

Database integrity

Referential and entity integrity ensure logical consistency.

CIA Triad: Availability



Availability

Availability means systems or information must be available on demand according to agreed-upon parameters.

CIA Triad: Availability

Threats to availability include:

Malicious attackers
(DDoS and ransomware)

Supply system failures
(Power outage and Internet downtime)

Device or system failures
(System crash)

Environmental issues
(Fire, earthquake, and tornadoes)

CIA Triad: Availability

The following are some countermeasures to ensure availability:

High availability

Ensure system availability at all times

Backup procedures

Ensure data restoration after a disaster

Security devices

Prevent DoS/DDoS attacks by deploying intrusion prevention system (IPS) and web application firewall (WAF)

Quick Check

You are working as a web architect, designing a new website using multiple small web servers behind a load balancer. What principle of information security are you enforcing?

A. Denial

B. Confidentiality

C. Integrity

D. Availability

Overview of IT Security

IT Security

It refers to the practice of protecting an organization’s information technology systems and data from threats such as unauthorized access, data breaches, and cyberattacks.

It aligns security strategies with the organization's goals, mission, and objectives to protect business operations from security risks while achieving desired outcomes.

IT Security with Organizational Goals, Mission, and Objectives

1

Goals:
Define what the organization desires to achieve

2

Mission:
Help in creating long term and short-term strategies

3

Objectives:
Indicate how it will proceed to achieve them

Aligning IT Security with Goals, Mission, and Objectives

It can be aligned with organizational goals, mission, and objectives in the following ways:

Reducing risk

- It involves protecting the organization's assets and processes through appropriate activities and controls.
- It makes one aware of IT assets and goals, mission, and objectives of the organization.

Senior management support

- It aids security professionals to be involved in and influence the organization's core activities.
- It also helps to identify priority tasks and divert resources to achieving security goals.

Overview of Control Framework

Control Framework

It is a data structure that comprises a set of an organization's internal controls, which includes the practices and strategies built to enhance business processes and minimize risk.

It is a set of controls that protects data within the IT infrastructure of a business or another entity.

It acts as a comprehensive security protocol that protects against fraud or theft from a spectrum of outside parties, including hackers and other kinds of cyber criminals.

Examples

- COBIT (Control Objectives for Information and Related Technologies)
- ISO 17799/27001

Control Framework

Examples of a control framework can be seen here:

Function Identifier	Function	Category Identifier	Category
ID	**Identify**	ID.AM	Asset management
		ID.BE	Business environment
		ID.GV	Governance
		ID.RA	Risk management
		ID.RM	Risk management strategy
		ID.SC	Supply chain risk management
PR	**Protect**	PR.AC	Identify management and access control
		PR.AT	Awareness and training
		PR.DS	Data security
		PR.IP	Information protection process and procedures
		PR.MA	Maintenance
		PR.RT	Protective technology

Control Framework

Function Identifier	Function	Category Identifier	Category
DE	**Detect**	DE.AE	Anomalies and events
		DE.CM	Security continuous monitoring
		DE.DP	Detection processes
RS	**Respond**	RS.RP	Response planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	**Recover**	RC.RP	Recovery planning
		RC.IM	Improvements
		RC.CO	Communications

Overview of Security Frameworks and Standards

Security Frameworks and Standards

The CISSP certification emphasizes various security frameworks and standards that are essential for designing, managing, and governing information security programs.

The following are the key security frameworks and standards commonly referenced in CISSP:

- ISO/IEC 27000 Series
  ISO/IEC 27001
  ISO/IEC 27002
- COBIT (Control Objectives for Information and Related Technologies)
- PCI DSS (Payment Card Industry Data Security Standard)
- NIST (National Institute of Standards and Technology) Frameworks

ISO/IEC 27001:2022

ISO 27001 is an international standard that outlines the requirements for an information security management system, helping organizations establish, implement, maintain, and continuously enhance their information security practices.

- 14 security domains are reduced to four domains.
- 114 controls are reduced to 93 controls.
  - 57 controls are merged.
  - 11 controls are added.
  - Three controls are deleted.
  - 35 controls remain unchanged.

S.No	Domains	Controls count
1	Organizational controls	37
2	People controls	8
3	Physical controls	14
4	Technological controls	34

ISO/IEC 27002:2022

- It provides guidelines for organizational information security standards and management practices, including the selection and implementation of controls.
- It considers the organization's information security risk environment when managing these controls.

It is designed to be used by organizations that intend to:

- Select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001
- Implement commonly accepted information security controls
- Develop their own information security management guidelines

Control Objectives for Information and Related Technologies (COBIT)

It is issued by ISACA® (Information Systems Audit and Control Association) and helps companies map their IT process to ISACA® best practices and standards.

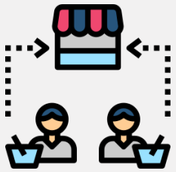
COBIT principles

- Meeting stakeholder needs
- Covering the enterprise end-to-end
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

Payment Card Industry Data Security Standard (PCI DSS)

It is an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data.

Visa, MasterCard, and American Express established PCI DSS as a security standard.



All organizations or merchants that accept, transmit, or store cardholder data, regardless of the size or number of transactions, must comply with this standard.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS merchant levels	
PCI DSS merchant level 1	>6 million transactions/year
PCI DSS merchant level 2	1 – 6 million transactions/year
PCI DSS merchant level 3	20,000 – 1 million transactions/year
PCI DSS merchant level 4	<20000 transactions/year

PCI DSS Requirements

The following are the criteria to be considered:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for passwords or other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Protect all systems against malware and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to cardholder data
- Identify and authenticate access to system components
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

NIST 800-53

It is a framework developed by NIST for securing information systems.

Goal: Safeguard organizations from cyberattacks, natural disasters, and human errors. While non-federal organizations are not required to adhere to it, they may need to do so as part of a contract or agreement with federal organizations.

It is designed to be used by federal organizations that intend to:

- Design to protect information systems from potential threats
- Reduce the risk of security incidents and improve overall security posture
- Be compliant with US federal government standards
- Allow customization to suit specific organizational needs
- Enhance the protection of sensitive information

Due Care

It is a legal term that pertains to the legal duty of the organization. Lack of due care is considered negligence.

Due care shows that a company has taken:

Responsibility for the activities that take place within the corporation

Necessary steps to protect the company, its resources, and its employees from possible threats

Reasonable care in protecting the organization

Due Care: Examples

Training employees in security awareness

Mandating statements from the employees stating that they have read and understood appropriate computer behavior

Deploying firewalls in the organization

Due Diligence

It is the act of understanding and investigating the risks the company faces and might not be legally liable.

- It means practicing the activities that maintain the due care efforts.
- It pertains to the best practices that a company should follow.

Due Diligence: Examples

Ensuring that the security controls are regularly monitored and frequently updated

In the case of firewalls, regularly monitoring security controls and updating rules depending on the requirement

Quick Check

A company is reviewing its policies and practices to ensure effective oversight and direction of its information security initiatives. What primarily drives information security governance in this context?

A. Regulatory requirements

B. Security policies

C. Business strategy

D. Threat assessment

Legal and Regulatory Issues Pertaining to Information Security

Cybercrimes

These are offenses committed with criminal intent to harm an individual's or group's reputation or cause physical or mental harm directly or indirectly.

These crimes are carried out using modern telecommunication networks, such as the Internet, through chat rooms, emails, notice boards, groups, and cell phones through SMS or MMS.

Computer Crimes

It involves a computer and a network.

Computer-related crimes have increased due to the:

- Connectivity of the Internet
- Low costs of computational resources

Examples

Cracking, copyright infringement, child pornography, and child grooming

Categories of Computer Crimes

These are criminal activities carried out using computers as mere tools and are not specific to computers.

Computer-assisted crime

Computer as target of crime

Computer incidental to crime

Examples

Fraud, distributed denial of service attacks, counterfeit, theft, and child pornography

Note:

80% of all criminal investigations include evidence that is digital in nature.

Categories of Computer Crimes

These are criminal activities focused on systems, servers, networks, and the data stored on these systems.

Computer-assisted crime

Computer as target of crime

Computer incidental to crime

Examples

Sniffing, denial of service, password attacks, viruses, digital identity theft, and computer hacking

Note:

These crimes target information systems and the underlying architecture.

Categories of Computer Crimes

In these types of crimes, the computer is related or incidental to the crime.

Computer-assisted crime

Computer as target of crime

Computer incidental to crime

Examples

Logging and recording of the list of customers for traffickers or online activities, whether based on the Internet or cell phones

Note:

These crimes occur without the use of computers.

Legislative Concepts

It refers to the systems of rules and legal principles that govern relationships and regulate behaviors within societies.

- International law
- Federal laws
- State law
- Common law
- Criminal law
- Tort law
- Administrative law
- Privacy law
- Restatement (second) of conflict of laws

Legislative Concepts

- **International law**
- Federal laws
- State law
- Common law
  - Criminal law
  - Tort law
  - Administrative law
- Privacy law
- Restatement (second) of conflict of laws

It is a complex system of rules governing relationships between states, international organizations, and individuals.

It is derived from:

- Treaties
- Customs
- International organizations
- General principles of law

Legislative Concepts

- International law
- **Federal laws**
- State law
- Common law
- Criminal law
- Tort law
- Administrative law
- Privacy law
- Restatement (second) of conflict of laws

These laws govern the entire country.

Example

- If a person robs a bank, they commit a federal crime and are therefore subject to federal prosecution and punishment.
- However, such cases are often handled by the states, as they have their own prescribed laws for such offenses.

Generally, the issues of jurisdiction and subsequent prosecution are worked out in advance between law enforcement and court jurisdictional bodies.

Legislative Concepts

- International law
- Federal laws
- **State law**
- Common law
  - Criminal law
  - Tort law
  - Administrative law
- Privacy law
- Restatement (second) of conflict of laws

It refers to the law of each state in the United States.

Examples

Speed limits, state tax laws, and criminal code

Note:

Federal laws are usually more comprehensive and may often supersede state laws.

Legislative Concepts

- International law
- Federal laws
- State law
- **Common law**
  - Criminal law
  - Tort law
  - Administrative law
- Privacy law
- Restatement (second) of conflict of laws

Legal systems in countries like the United States, Canada, and the United Kingdom emphasize on determinant of laws and sets a judicial precedent.

It has three branches of law:

- Criminal law
- Civil law or tort law
- Administrative or regulatory law

Legislative Concepts

- International law
- Federal laws
- State law
- **Common law**
  - **Criminal law**
  - Tort law
  - Administrative law
- Privacy law
- Restatement (second) of conflict of laws

It addresses behavior that is harmful to society.

It includes punishments, such as monetary fines, imprisonment, and death.

It is the prosecution’s responsibility to prove guilt beyond a reasonable doubt.

Legislative Concepts

- International law
- Federal laws
- State law
- **Common law**
  - Criminal law
  - **Tort law**
  - Administrative law
  - Privacy law
  - Restatement (second) of conflict of laws

It is a body of rights, obligations, and remedies that sets out reliefs for persons suffering harm due to the wrongful acts of others.

Tort actions are not dependent on an agreement between the parties involved in a lawsuit.

Tort law serves four objectives:

- Compensates victims for injuries suffered by the culpable action or inaction of others
- Shifts the cost of injuries to the person or persons responsible for inflicting them
- Discourages injurious, careless, and risky behavior in the future
- Vindicates legal rights and interests that are compromised, diminished, or emasculated

Legislative Concepts

- International law
- Federal laws
- State law
- **Common law**
  - Criminal law
  - Tort law
  - **Administrative law**
- Privacy law
- Restatement (second) of conflict of laws

These are laws and legal principles that address several areas.

These include:

- International trade
- Manufacturing
- Environment
- Immigration

Legislative Concepts

- International law
- Federal laws
- State law
- Common law
- Criminal law
- Tort law
- Administrative law
- **Privacy law**
- Restatement (second) of conflict of laws

It includes language indicating that personal information must be destroyed when its retention is no longer required.

Privacy is the right of an individual to determine when, how, and to what extent one releases personal information.

Legislative Concepts

- International law
- Federal laws
- State law
- Common law
- Criminal law
- Tort law
- Administrative law
- Privacy law
- **Restatement (second) of conflict of laws**

It is the basis for deciding which laws are more appropriate when there are conflicting laws in different states.

The conflicting legal rules come from US federal laws, the laws of the states of the United States, or the laws of the other countries.

Intellectual Property (IP) Law

It is designed to protect both tangible and intangible items and properties from those who want to copy or use them without due compensation to the inventor or creator.

IP law categories

Industrial property

Inventions or patents, trademarks, industrial designs, and geographical indications of source

Copyright

Novels, poems, plays, films, musical works, drawings, paintings, photographs, and sculptures and architectural designs

Types of Intellectual Property (IP) Law: Patent

Patent

It grants the owner a legally enforceable right to exclude others from practicing the invention.

It is applicable for 20 years.

It protects new, useful, and nonobvious inventions.

After the expiry of a patent, the invention is open to the public domain.

Types of Intellectual Property (IP) Law: Patent

To receive a patent, the following three requirements must be satisfied:

The invention should be new and an original idea.

The invention must be useful.

The invention must not be obvious.

Types of Intellectual Property (IP) Law: Trademark

Trademark

It protects the goodwill a merchant or vendor invests in the products.

It grants exclusive rights to the owner of the trademark.

It consists of any word, name, symbol, color, sound, product shape, device, or a combination of these.

It is registered with a government registrar.

Types of Intellectual Property (IP) Law: Trademark

A trademark must adhere to the following conditions:

One trademark must not be similar to another trademark.

The trademark should not be descriptive of the goods or services that one offers.

Types of Intellectual Property (IP) Law: Copyright

Copyright

It covers the expression of ideas and usually protects artistic properties, such as writing, recordings, databases, and computer programs.

The duration of protection is longer.

Works of one or more authors are protected until 70 years after the death of the last surviving author.

Anonymous works are protected for 95 years from the first publication or 120 years from creation, whichever is shorter.

Types of Intellectual Property (IP) Law: Copyright

Digital Millennium Copyright Act (DMCA)

- It is a controversial US DRM law designed to update copyright laws to address the challenges of regulating digital material.
- Nonprofit organizations are exempted from this act.

DMCA takedown notice

- It is a notice given to a web host or search engine, informing them that they are hosting or linking to copyright-infringing material.
- It provides them a notice to remove the copyrighted works.

Types of Intellectual Property (IP) Laws: Trade Secret

Trade secret

It is something that is proprietary to a company and important for its survival and profitability.

The trade secret law protects certain types of information or resources from unauthorized use or disclosure.

Trade secrets can be protected by implementing control structures depending on the type of trade secret and by making the employees sign an NDA.

Example

The formula used for a soft drink such as Coke or Pepsi, a new form of mathematics, the source code of a program, or a method of making the perfect jellybean

Types of Intellectual Property (IP) Laws: Licenses

Licenses

Software licenses are a contract between the provider of a software and the consumer.

The four categories of software licensing are:

- **Contractual license agreement:** It is a written contract between the software vendor and the customer.
- **Shrink-wrap license:** A shrink-wrap license is an end-user agreement (EULA) that is enclosed with a software in a plastic-wrapped packaging. Once the end-user opens the packaging, the EULA is in effect.
- **Clickwrap license:** This type of agreement is often used in connection with software licenses. Most clickwrap agreements require the end-user to manifest his or her assent by clicking an OK or agree button on a dialog box or a pop-up window.
- **Cloud services license agreement:** It is similar to a clickwrap agreement and is mainly concentrated on the services provided by cloud vendors.

US Computer Laws

Computer Fraud and Abuse Act (CFAA) of 1986

- It is a United States legislation that criminalizes unauthorized access to classified or financial information in a federal system.

Computer Security Act of 1987

- It improved the security and privacy of sensitive information in federal computer systems by setting minimally acceptable security practices.
- It mandated baseline security for federal agencies and made the National Institute of Science and Technology (NIST) responsible for developing standards and guidelines.

US Computer Laws

Federal Sentencing Guidelines 1991

- It provides punishment guidelines to help federal judges interpret computer crime laws.
- It is a prudent man rule that requires senior executives to take personal responsibility for ensuring due care.

Federal Information Security Management Act (FISMA)

- It defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats.
- It requires agencies to implement an information security program that covers the agencies' operations and contractors.
- It requires contractors to be a part of the scope and makes NIST responsible for building FISMA guidelines.

Import or Export Controls and Transborder Data Flow

Organizations must ensure compliance with import or export controls and understand transborder data flow regulations to navigate international laws and safeguard cross-border data transfers.

Import or export controls

- They ensure that software complies with the local laws.
- Certain applications, like encryption software, are illegal to import or export.
- The UNSC can impose sanctions on any country, strictly prohibiting technology transfers to these countries.

Transborder data flow

- It involves the transfer of data from one country to another.
- An information security professional must understand data jurisdiction during cross-border transfers.

Offshoring: Privacy Requirements and Compliance

It involves outsourcing to another country, which may lead to increased privacy and regulatory issues.

Example

Data offshored to India by a US medical transcription organization is less secure.

- Health Insurance Portability and Accountability Act (HIPAA) certification is a major regulation covering healthcare data in the United States.
- A good contract ensures that regulations and laws governing privacy are followed both in and beyond a country's jurisdiction.

Example

The Indian company to which the US Medical Transcription organization's data is offshored can agree to follow HIPAA rules via a contract.

Introduction to Privacy

It is the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

The need for more privacy laws and governance has increased due to:

- Data aggregation and advancement of retrieval technologies
- Loss of borders
- Advancement of convergent technologies

Privacy Terms

Personal Identifiable Information (PII)

- It is any data that could potentially identify a specific individual.
- Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Personal Health Information (PHI)

- It is any health-related information that can be related to a specific person.
- In the United States, HIPAA mandates the protection of PHI.

Types of Privacy Regulations

Local or regional

- They vary based on cultural, social, and legal factors.

Example

The California Consumer Privacy Act (CCPA) gives Californians more control over personal data and privacy.

National

- They set privacy rights and obligations for organizations within entire countries.

Example

In the United States, HIPAA protects healthcare data privacy.

Global

- They set a global data protection standard for organizations processing EU citizens' data.

Example

ISO 27701 offers a framework for managing privacy information systems.

US Privacy Laws

4th Amendment to US Constitution

- People's right to security in their homes, papers, and possessions is protected against unreasonable searches and seizures.
- Warrants are issued only for probable cause and must specify the location.

Federal Privacy Act of 1991

- It codifies data protection for US citizens used by the federal government.
- It outlines how information can be used, collected, and distributed.
- It forbids federal agencies from sending private information without consent.

US Privacy Laws

Electronic Communication Privacy Act (ECPA)

- It criminalizes invading an individual's electronic privacy.
- It broadened the Federal Wiretap Act.
- It restricts the government from putting wiretaps on phone calls and other electronic communications.

Stored Communication Act (SCA)

- It was enacted in the United States in 1986 as part of ECPA.
- It protects certain electronic communications and computing services from unauthorized access or interception.
- It is now applicable to social media.

US Privacy Laws

USA Patriot Act of 2001

- It stands for uniting and strengthening America by providing tools required to intercept and obstruct terrorism.
- It allows searches and seizures to be carried out without immediate notification of the person.
- It amends the Computer Fraud and Abuse Act to strengthen penalties for those convicted.

Children's Online Privacy Protection Act

- It applies to US websites collecting privacy information from children under the age of 13.
- It mandates the websites to have a privacy notice stating the information collected, its use, and any third-party disclosure.
- It ensures that parents give verifiable consent before collecting data about children under the age of 13.

US Privacy Laws

The Gramm-Leach-Bliley Act of 1999 (GLBA)

- It applies to financial institutions and is driven by the Federal Financial Institutions Examination Council (FFIEC).
- Enacted in 1999, it requires safeguarding consumer financial information.
- It mandates financial institutions to develop privacy notices and allow customers to opt out of information sharing.
- It makes the board of directors responsible for any security issues.
- It mandates financial institutions to have a written security policy in place.

Sarbanes–Oxley Act of 2002

- It is directly related to the financial scandals in the late 90s.
- It is a regulatory compliance standard for financial reporting.
- It imposes criminal penalties for intentional violations.
- It ensures that firms provide real-time disclosures of any events that may affect a firm price or financial performance.

US Privacy Laws

Health Insurance Portability and Accountability Act (HIPAA)

- It is a US federal regulation standardizing the storage, use, and transmission of personal medical and healthcare data.
- It provides a framework and guidelines to ensure security, integrity, and privacy.
- It mandates steep federal penalties for noncompliance.
- A business associate (BA) is a person or entity that handles PHI for a covered entity.
- A business associate agreement (BAA) protects PHI as per the HIPAA guidelines.

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

- It was passed in 2009 by Congress as an amendment to HIPAA.
- It changed the way the law treated Bas and organizations that handled PHI.
- It also introduced new data breach notification requirements.
- It mandates HIPAA-covered entities to notify affected individuals of a data breach and inform the Secretary of Health and the media if over 500 people are affected.

Safe Harbor Privacy Principles

They were designed to prevent private organizations in the European Union or the United States from accidentally disclosing or losing personal information about customers.

They were developed between 1998 and 2000.

The department of commerce of the United States is responsible for Safe Harbor.

Safe Harbor Principle

US companies could opt into a program and be certified if they adhered to the following seven principles:

1. Notice
2. Choice
3. Onward Transfer
4. Security
5. Data Integrity
6. Access
7. Enforcement

Privacy Shield and Transatlantic Data Privacy Framework (TDPF)

Privacy Shield

- The European Court of Justice invalidated the International Safe Harbor Principles in 2015, replacing them with the EU-US Privacy Shield.
- Since August 2016, organizations started self-certifying to Privacy Shield, an improved framework.

Transatlantic Data Privacy Framework (TDPF)

- It is a proposed agreement between European Union and the United States that facilitates the transfer of personal data from European Union to the United States.
- It is intended to replace the Privacy Shield Framework, which the Court of Justice of the European Union (CJEU) invalidated in 2020.

OECD Privacy Principles

The Organization for Economic Cooperation and Development (OECD) is a group of 34 member countries that discuss and develop economic and social policies. It ensures:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation

OECD Privacy Principles

The OECD published a set of revised guidelines governing the protection of privacy and transborder flows of personal data. The guidelines ensured:

Security safeguards

Openness

Individual participation

Accountability

General Data Protection Regulation (GDPR)

It is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within the European Union.

Companies collecting data on EU citizens must comply with strict data protection rules starting May 25, 2018.

Noncompliant organizations face fines of up to €20 million or 4% of their global turnover, whichever is higher.

General Data Protection Regulation (GDPR)

Organizations must report data breaches within 72 hours.

Companies must also allow users to export their data and delete it.

Under the **right to be forgotten,** individuals can request companies to remove certain online data about them.

Data Protection Principles

The **EU General Data Protection Regulation (EU GDPR)** outlines six data protection principles that organizations need to follow for collecting, processing, and storing individuals' personal data.

Lawfulness, fairness, and transparency

Purpose limitation

Data minimization

Accuracy

Storage limitations

Integrity and confidentiality

The data controller is responsible for complying with the principles and must be able to demonstrate the organization's compliance practices.

EU GDPR: Roles and Responsibilities

A **data subject** is an identifiable natural person who can be identified by attributes such as a name, an identification number, or other factors related to their identity.

A **data controller** is the legal entity that either alone or jointly determines the purpose for and way personal data is, or will be, processed.

A **data processor** processes data on behalf of the data controller but does not control the data and cannot change the purpose or use of the particular set of data.

A **supervisory authority (SA)** is established in each EU member state to enforce and monitor the application of GDPR rules to protect individual rights for the processing and transfer of personal data within the European Union.

Quick Check

A researcher is preparing to file a patent for a new invention and is reviewing the necessary criteria for patentability. Which of the following requirements is NOT needed for an invention to be considered patentable?

A. Novel

B. Useful

C. Inventive step

D. Obvious

Requirements for Investigation Types

Investigation

"An investigation is a fact-finding process of logically, methodically, and lawfully gathering and documenting information for the specific purpose of objectively developing a reasonable conclusion based on the facts learned through the process."

~ ANSI/ASIS INV.1-2015 Investigation Standards

The purpose of an investigation is to:

Identify and collect evidence

Determine what happened

Determine who is responsible

Investigation Types

Criminal investigation

Civil investigation

Administrative investigation

Regulatory investigation

Investigation Types: Criminal Investigation

01

It involves determining whether a criminal law has been violated.

It is usually conducted by law enforcement organizations.

02

03

Criminal cases involve an action that is harmful to society.

Punishment usually involves jail time, monetary fines, or sometimes capital punishment.

04

Investigation Types: Civil Investigation

It deals with offense committed against individuals or companies that result in damages or loss.

Punishment usually involves recovering money to compensate the victim for damages.

Investigation Types: Administrative Investigation

It is conducted by local management in response to complaints or concerns that generally are personnel related and non-criminal in nature.

It may be initiated in response to complaints, mishaps, misconduct, or violations of the organization’s policy.

If evidence reveals any malicious or criminal activities, it could trigger criminal or civil investigations.

Investigation Types: Regulatory Investigation

It involves determining whether a regulatory law has been violated.

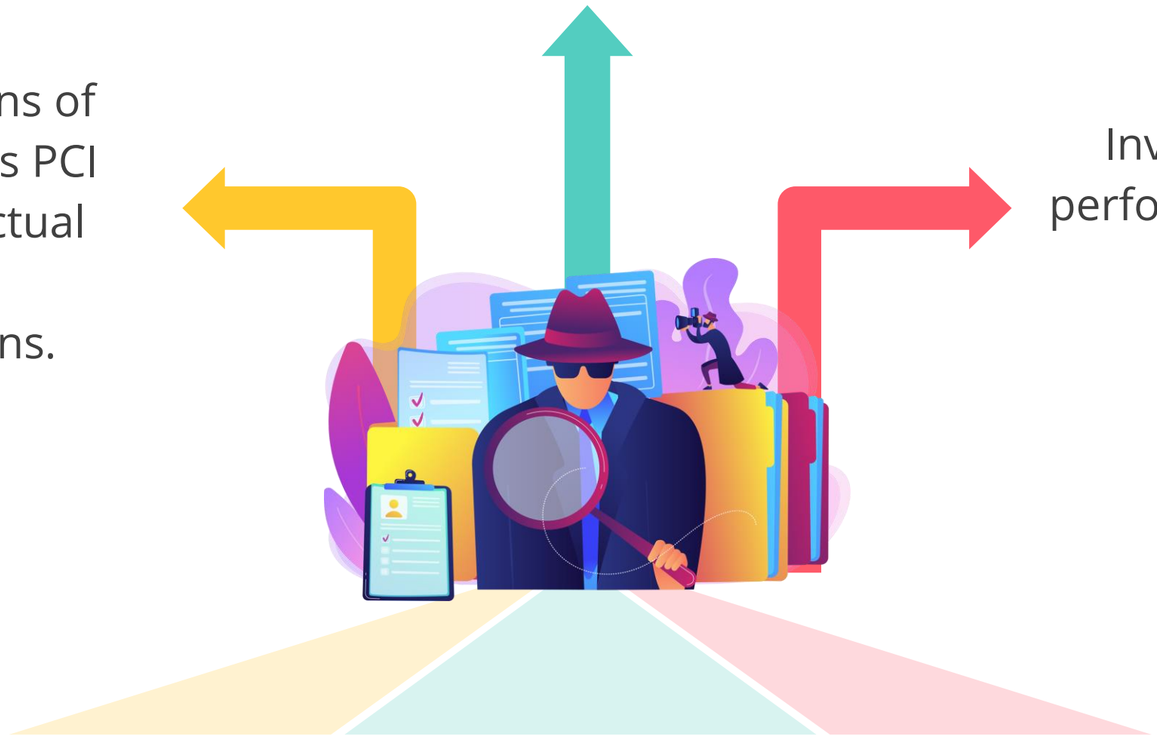
Regulation is a law established by the government body.

Initial inquiries can vary from a simple phone call for basic information to a formal regulatory investigation with subpoenas for detailed answers.

Investigation Types: Industry Standards

Penalties may lead to fines or other sanctions.

Investigations into violations of industry standards (such as PCI DSS) are based on contractual obligations between participating organizations.



Investigations may be performed by independent third-party.

Quick Check

In a legal seminar, participants are discussing the consequences of various legal violations. How should the punishments be matched for violations of criminal law, civil law, and regulatory law?

A. Financial restitution, prison sentence, and financial penalty

B. Prison sentence, financial restitution, and financial penalty

C. Financial penalty, prison sentence, and financial restitution

D. Prison sentence, financial penalty, and financial restitution

Implementing Security Policies, Standards, and Procedures

Security Management Plan (SMP)

It is a comprehensive document that outlines the strategies, policies, procedures, and resources an organization should employ to protect its information assets.

It serves as a roadmap for implementing and maintaining effective information security measures.

Security Plan Components

Security policies

Standards

Guidelines

Procedures

Baselines

Organization structure

The top management is responsible for policies, and the mid-level management is responsible for developing standards, guidelines, and procedures aligned with the security policies.

Approaches to Security Plan

There are several approaches to developing an SMP and the most common and effective ones include:

Top-down approach

- Management initiates the security policy, which is passed down to operations staff.
- Top-level managers are responsible for implementing data protection strategy, including policy creation, procedures, and escalation plans.
- It is more successful when compared to the bottom-up approach.

Bottom-up approach

- Operational staff initiate the process and propose policies to management.
- This approach has occasionally resulted in problems due to management not being fully aware of things.
- It uses a person or team's experience and expertise to handle security concerns.

Security Management Plan Types

Strategic plan

- Long term plan
- Defines the goals of the entire organization with a holistic approach
- Effective for at least five years and reviewed annually
- **Example:** To protect patient data and ensure compliance with HIPAA regulations

Senior management

Tactical plan

- Means to activate a strategy
- Mid-term plan developed to provide more detailed goals
- Typically spans one to two year and is technology-oriented
- **Examples:** Project plans, acquisition plan, budget plan, and hiring plan

Middle management

Operational plan

- Short-term plan with specific results expected from departments and workgroups
- Highly-detailed plan
- Updated often (monthly or quarterly)
- **Examples:** Resource allotment, budgetary allocation, and training plans

Implementation team

Security Policy

It is a broad statement produced by the senior management that dictates the role of security within the organization.

The characteristics of security policies are:

It must integrate security into all business processes and functions.

It must support the vision and mission of the organization.

It must be generic, non-technical, and easily understood.

It must be reviewed and modified periodically or as the company environment changes.

Types of Security Policies

There are mainly three types of security policies:

Organizational security policy

It focuses on issues relevant to every aspect of the organization.

Issue-specific policy

It focuses on a specific service, department, or function that is distinct from the organization.

System-specific policy

It focuses on individual systems.

Security Policy Implementation

Policy documents often come with the endorsement or signature of the executive powers within an organization.

The following must be considered when implementing a security policy:

Policy enforcement

Policy elements

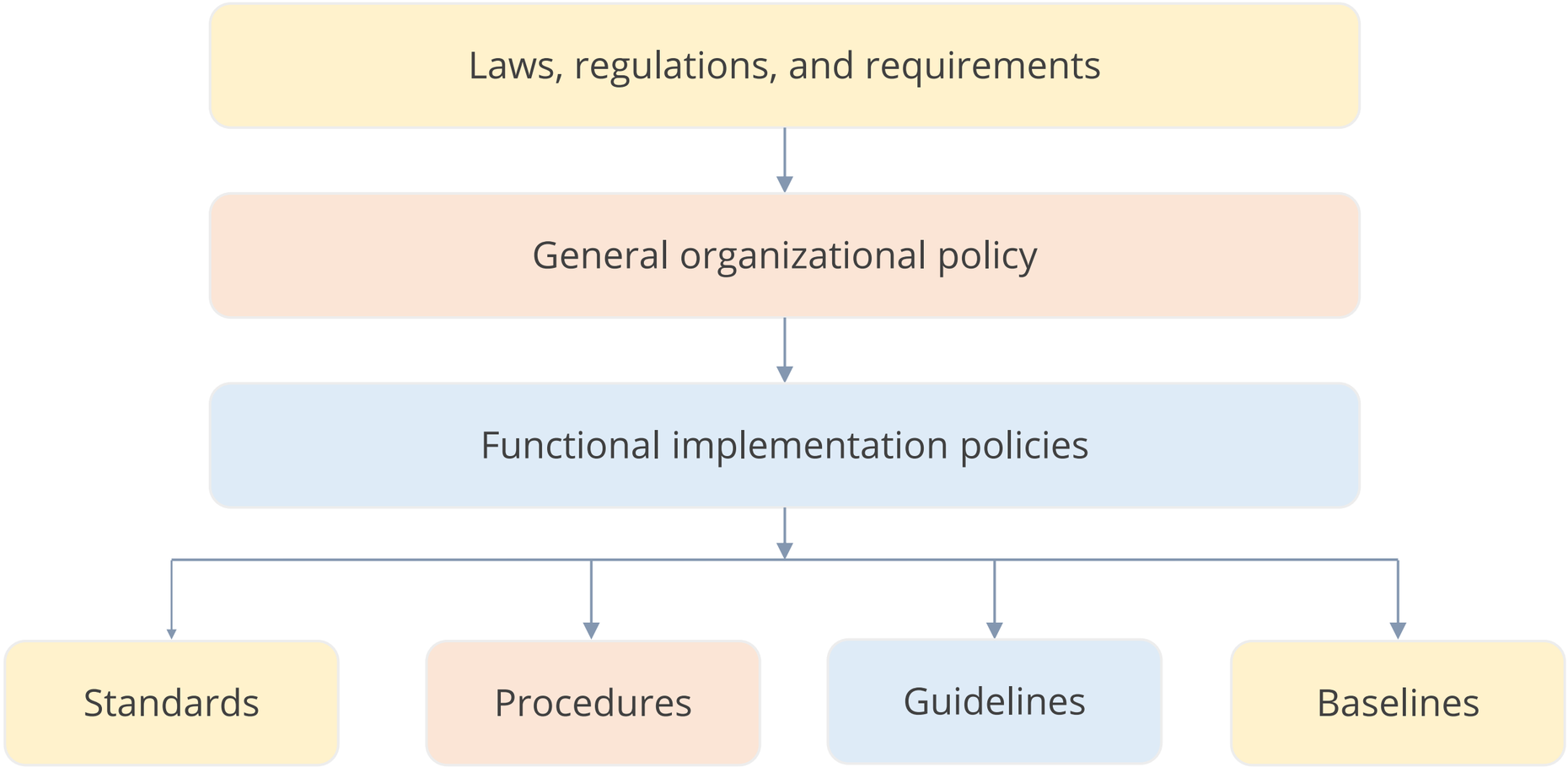
Management responsibilities for policy

Standard policy components

Policy creation guidelines

Policy Chart

A strategic goal can be viewed as the ultimate endpoint, while tactical goals are the steps necessary to achieve it.



Standards

These are established requirements or rules that describe the specific methods and practices to be followed.

The characteristics of security standards include the following:

Explains how to implement high-level guidelines operationally

Aligns security practices with industry best practices and regulatory requirements

Requires periodic review and modification or when related policies change

Supports security policies and organizational objectives

Procedures

These are a set of documented steps or guidelines designed to standardize and streamline process within an organization.

The characteristics of procedures include the following:

Provides clarity and consistency in tasks, decisions, and changes

Serves as a roadmap for daily operations, aligning with security goals

Requires regular updates due to technological changes

Includes flowcharts or diagrams written in a step-by-step format for clarity

Guidelines

It is a principle or instruction that helps people decide what to do or how to act in a particular situation.

The characteristics of security guidelines include the following:

They are discretionary in nature.

They provide a suggested course of action while allowing flexibility based on specific circumstances.

They are reviewed periodically or as needed per requirements.

They support security policies and organizational objectives.

Baseline

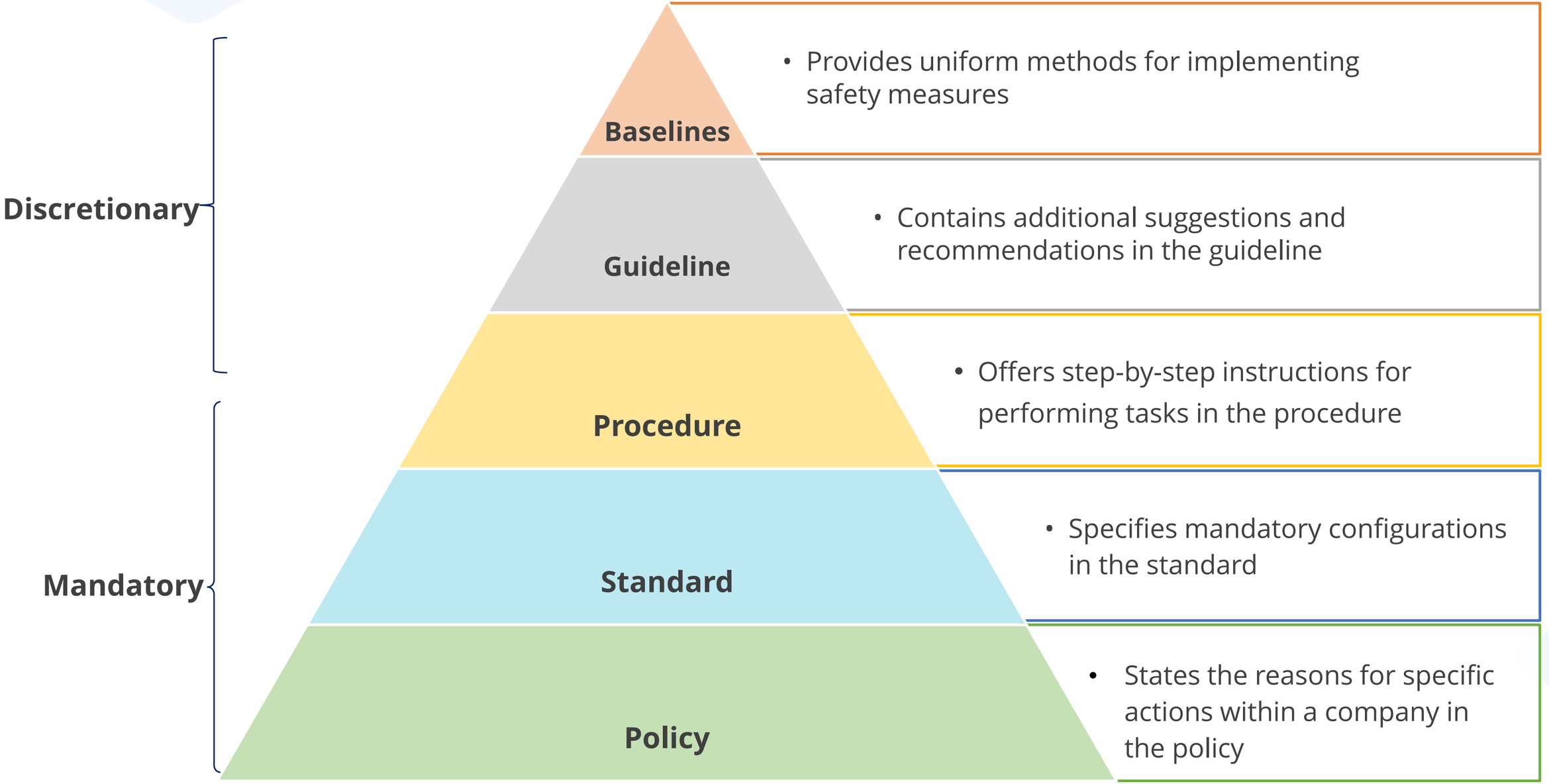
It is a predefined set of configurations and best practices meticulously designed to create a resilient and secure foundation for computing resources.

The characteristics of baseline include the following:

- Enforces consistent security practices across the organization to decisively reduce the risk of vulnerabilities
- Proactively identifies and neutralizes potential security threats by setting a benchmark for acceptable risk

- Streamlines security management processes and reduces the time and effort required to maintain a secure environment
- Helps in reducing risks by establishing a baseline for acceptable risk

Policy, Standard, Procedure, and Guideline



Policy, Standard, Procedure, and Guideline

	Policies	Standards	Procedures	Guidelines
Definition	A high-level statement of organizational senior management intent	A detailed description of how policies should be implemented	Detailed, step-by-step instructions for completing a task	Recommended best practices or advice for carrying out a task
Scope	Broad and organization-wide	Specific to a policy or area	Specific to task or process	Broad applicability, but not mandatory
Enforcement	Enforced through disciplinary actions or penalties	Enforced through compliance audits or certification processes	Enforced through training, monitoring, and corrective actions	Not enforced, but noncompliance may result in suboptimal outcomes
Review Frequency	Annually or in case of any change in business objectives	Periodic, based on policies or technology changes	Frequent, based on process changes	Periodic or as needed per requirements

Policy, Standard, Procedure, and Guideline

	Policies	Standards	Procedures	Guidelines
Style	Formal, concise, and authoritative	Technical, detailed, and precise	Step-by-step, with accompanying visuals or flowcharts	Narrative, with explanations and examples
Example	All employees and contractors must use strong passwords and follow secure management practices to protect organization's assets and systems.	Passwords must be at least 12 characters long and include a combination of upper case, lower letters, and special characters.	**To reset a portal:** 1. Visit the password reset portal 2. Enter your employee ID and email address 3. Answer the security questions	It is recommended to use a passphrase for the password.

Quick Check

During a discussion about organizational decision-making, the team is evaluating different actions that may or may not be required. Which of the following is most likely to be a discretionary action?

A. Policy

B. Procedures

C. Standard

D. Guidelines

Quick Check

An organization decides to replace its aging firewall from another vendor. Which of the following documents will undergo maximum and minimal changes?

A. Max: Policy, Min: Standard

B. Max: Policy, Min: Procedures

C. Max: Procedures, Min: Standard

D. Max: Procedures, Min: Policy

Identify, Analyze, and Prioritize Business Continuity (BC) Requirements

Business Continuity

It refers to a company’s ability to keep running and minimize disruptions during unexpected events, like natural disasters, cyberattacks, or power outages.

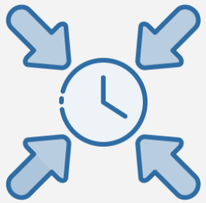
Need for Business Continuity Planning (BCP)

Business operations are interrupted by unexpected events. Companies must develop business continuity and disaster recovery plans to face these issues.

The focus areas of business continuity planning are:

- Protect the lives of employees

- Minimize the disruptions

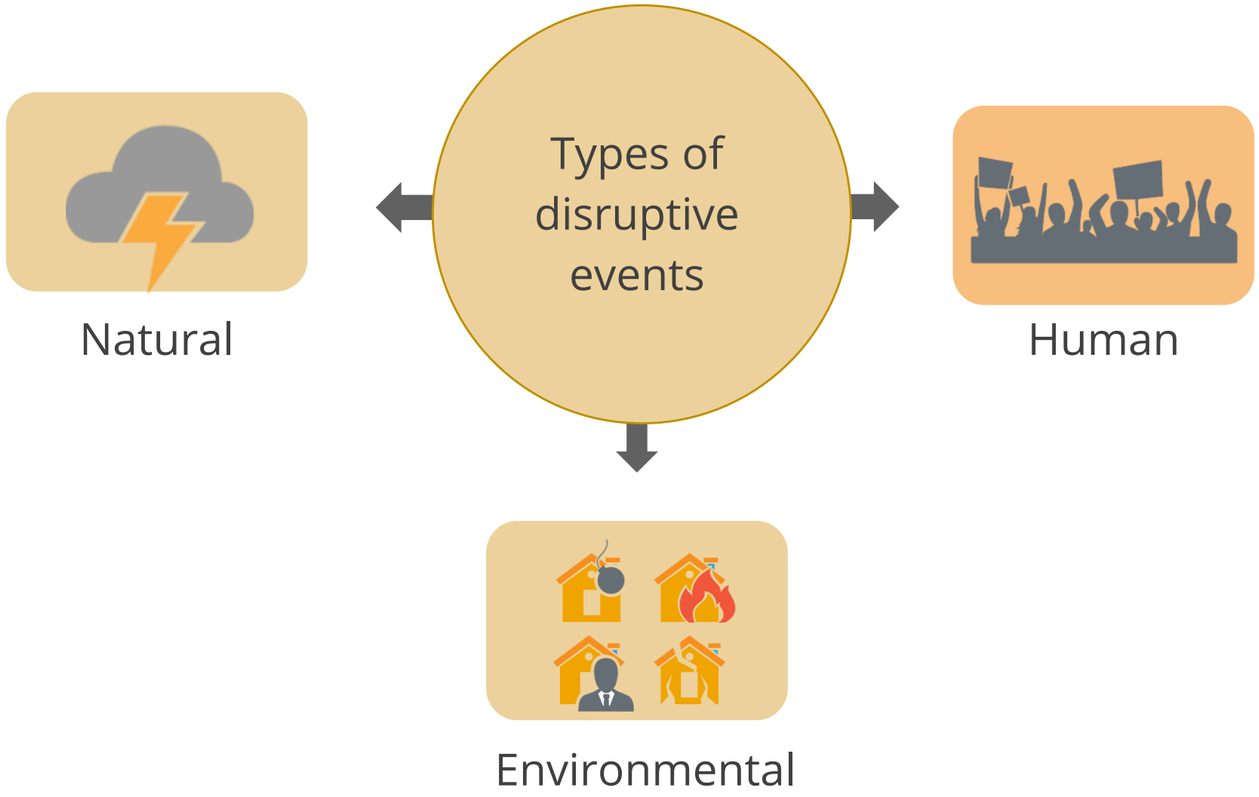


- Restore normal business

- Prevent financial losses

Basic Concepts: Disruptive Events

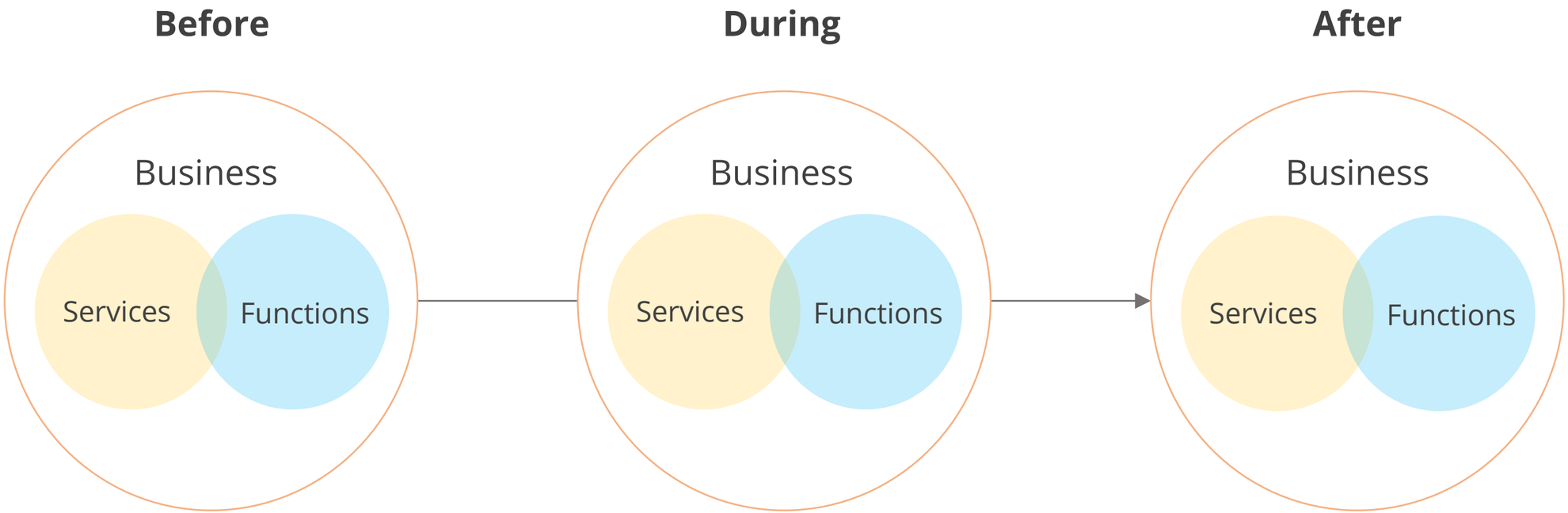
It is any incident, act, or occurrence that suspends normal operations.



Disruptive events can be intentional or unintentional, and a BCP aims at minimizing its effects on a company.

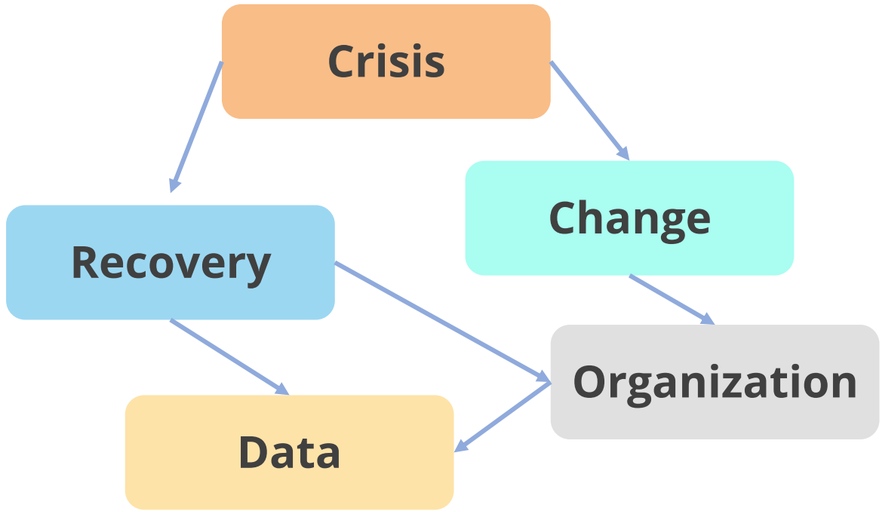
Basic Concepts: Business Continuity Planning

The goal of a BCP is to ensure business continuity before, during, and after a disaster strikes.



Importance of Business Continuity Planning

The organization’s ability to respond to any disaster and recover from disruptions depends on business continuity planning (BCP) or disaster recovery planning (DRP) as it:



Is the **last** line of defense for any organization against any threat

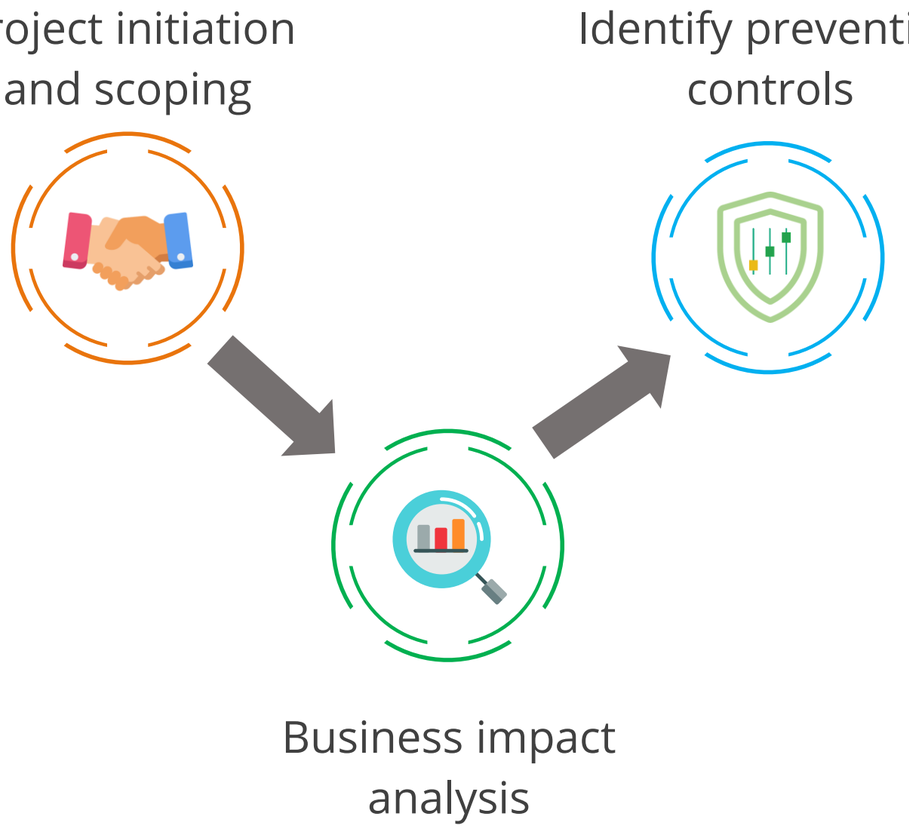
- Ensures all **planning** has been considered
- Helps **reduce the risks** faced by the organization

Example

Usage of cloud computing resources to safeguard data

Business Continuity Planning Phases

The high-level phases as per NIST 800-34 for achieving comprehensive BCP or DRP are:



BCP or DRP Phase 1: Project Initiation and Scoping

The following activities take place in this phase:

- Creating project scope and defining parameters
- Obtaining management’s support
- Identifying potential outages to critical systems for risk analysis to be performed
- Appointing project planner and selecting staff for plan development and execution
- Assigning the BCP or DRP project manager or coordinator as the key point of contact (POC)
- Ensuring the completions of BCP or DRP by Project Manager and testing it routinely
- Identifying the representatives of BCP committee from senior management, legal, CFO, systems and applications, business units, systems support, communications, data center, communications, and information security

BCP or DRP Phase 2: Business Impact Analysis (BIA)

It is the formal method of determining the impact of disruption to the organization's IT systems on the business and organization's processes and functions.

It enables the BCP or DR project manager to plan the requirements and priorities for IT contingencies by **identifying and prioritizing critical IT systems and components.**

BCP or DRP Phase 2: Business Impact Analysis (BIA)

It necessitates the analysis of the following internal and external environments:

External context

- Economic condition
- Political landscape
- Technological advancements
- Legal regulations
- Social trends
- Competitors actions

Internal context

- Strategic objectives
- Organizational structure
- Company cultures
- Resources
- Standards, guidelines, and models of the organization
- Contractual relationship

BCP or DRP Phase 2: Business Impact Analysis (BIA)

The three major goals of BIA are:

Criticality prioritization

- Identifying and prioritizing every critical business unit process
- Evaluating the impact of a disruptive event
- Assigning higher priority rating for time-critical business processes over non–critical business processes

Downtime estimation

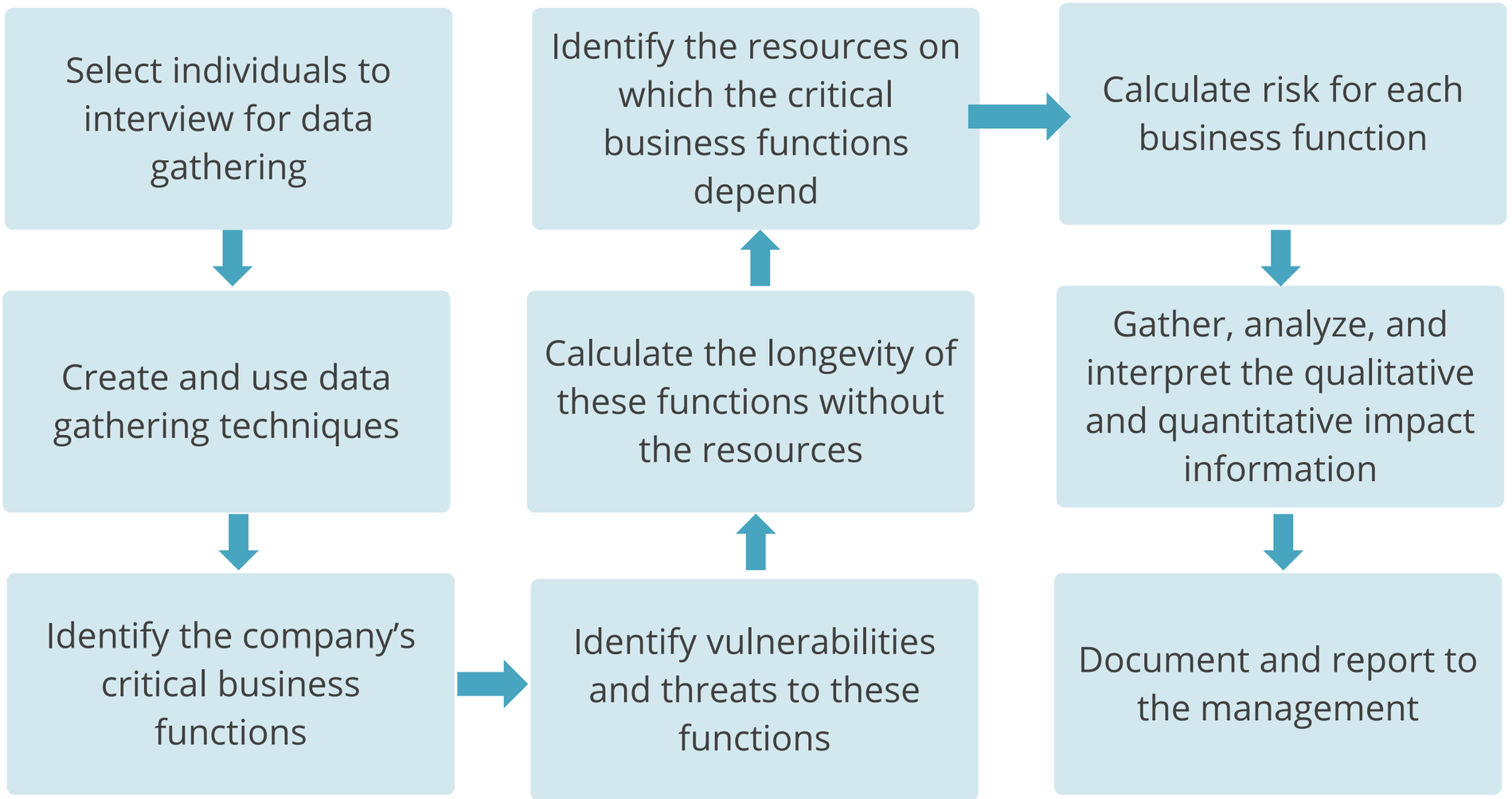
- Estimating Maximum Tolerable Downtime (MTD) using the BIA
- Determining the downtime required for the business to remain viable
- Identifying non-recovery if the interruption of a critical process extends the maximum tolerable downtime

Resource requirements

- Estimating resource requirements
- Allocating more resources to time-sensitive processes as compared to less critical processes

BCP or DRP Phase 2: Business Impact Analysis (BIA)

The steps of a BIA are outlined here:



BCP or DRP Phase 2: Business Impact Analysis (BIA)

For each major business unit within the organization, the following steps will be performed:

Identify business components or activities that, if disrupted or unavailable, could jeopardize the company's operations

Determine the required Maximum Tolerable Downtime (MTD)

Maximum Tolerable Downtime (MTD)

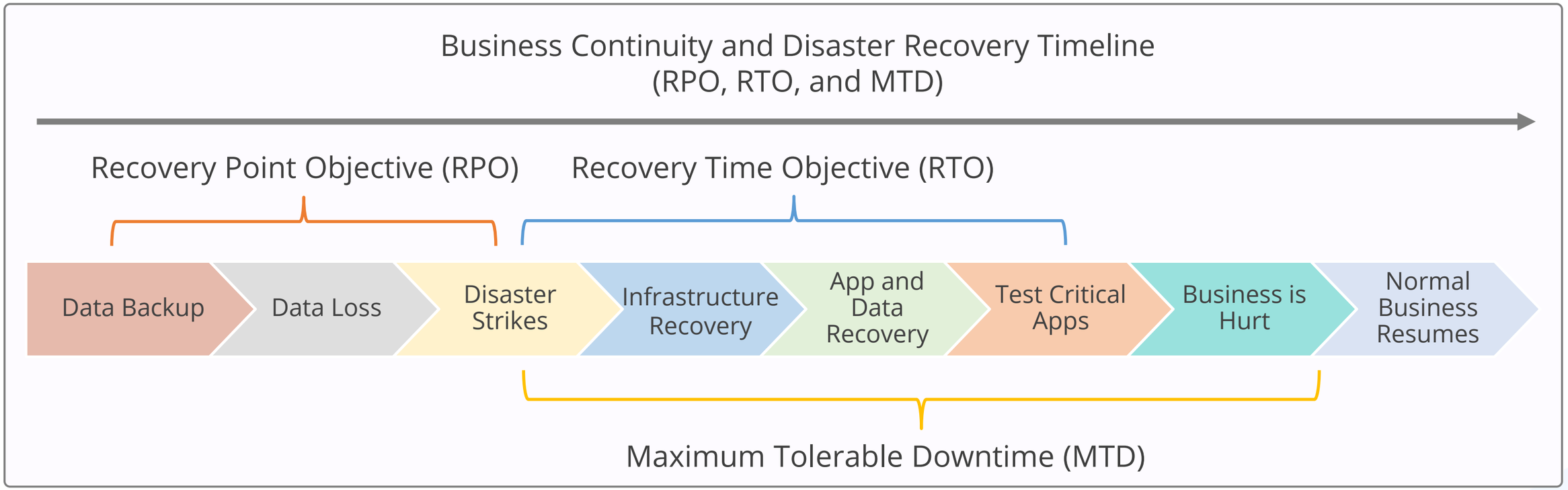
It is the maximum period for which the organization’s key processes and functions are unavailable, after which the organization would suffer significant losses.

It is measured in minutes, hours, days, or longer, depending on the nature of the business.

It is revised several times during the course of a project.

Maximum Tolerable Downtime (MTD)

The alternate terms for MTD include Maximum Allowable Downtime (MAD), Maximum Acceptable Outage (MAO), and Maximum Tolerable Outage (MTO).

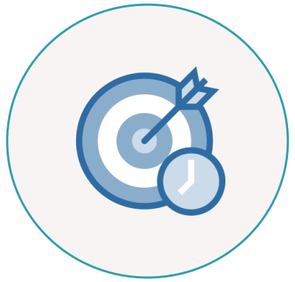


Failure and Recovery Metrics

A number of metrics are used to quantify the frequency of system failures.

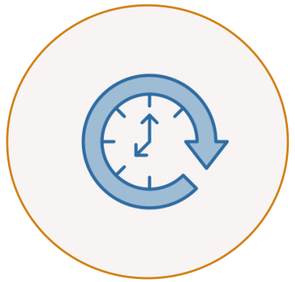
Recovery Point Objective

- Level of data, work loss, or system inaccessibility resulting from a disruptive event
- Usually expressed in units of time



Recovery Time Objective

- Maximum time allowed to recover business or IT systems
- Expressed in units of time such as minutes, hours, or days



Work Recovery Time

- Time required to configure a recovered system
- Consists of the system’s recovery time and the work recovery time

Failure and Recovery Metrics

A number of metrics are used to quantify the frequency of system failures.

Mean Time between Failures

- Predicted elapsed time between inherent failures of a system during operation
- Calculated as the arithmetic mean time between failures of a system

Mean Time to Repair

- Duration to recover a specific failed system
- Total corrective maintenance time divided by the total number of corrective maintenance actions during a given period

Minimum Operating Requirements

- Minimum environmental and connectivity requirements for a computer equipment to operate
- Documentation is important for each IT critical asset

Examples of RTO and RPO

An organization can accept data loss for up to four hours and cannot afford to have any downtime.

What is the RTO and RPO?

RTO is zero hours, and RPO is four hours.

An organization takes a data backup twice daily. The first backup is at 12 am and the second is at 12 pm.

What is the RPO?

Since a data backup is done every 12 hours, the maximum data loss is 12 hours. Hence, the RPO is 12 hours.

An organization takes a data backup three times a day. The first backup is at 8 am, the second is at 4 pm, and the third is at 12 am.

What is the RPO?

Since the data backup is done every eight hours, the maximum data loss is eight hours. Hence, the RPO is eight hours.

Examples of RTO and RPO

Following an incident, primary site systems went down at 3 pm and resumed from the alternate site at 6 pm, as per the defined RTO.

What is the RTO?

Since the system was down for three hours, the RTO is three hours.

The BCP mandates no data loss and service restoration within 36 hours for critical systems.

What is the RTO and RPO?

RTO is 36 hours, and RPO is zero hour.

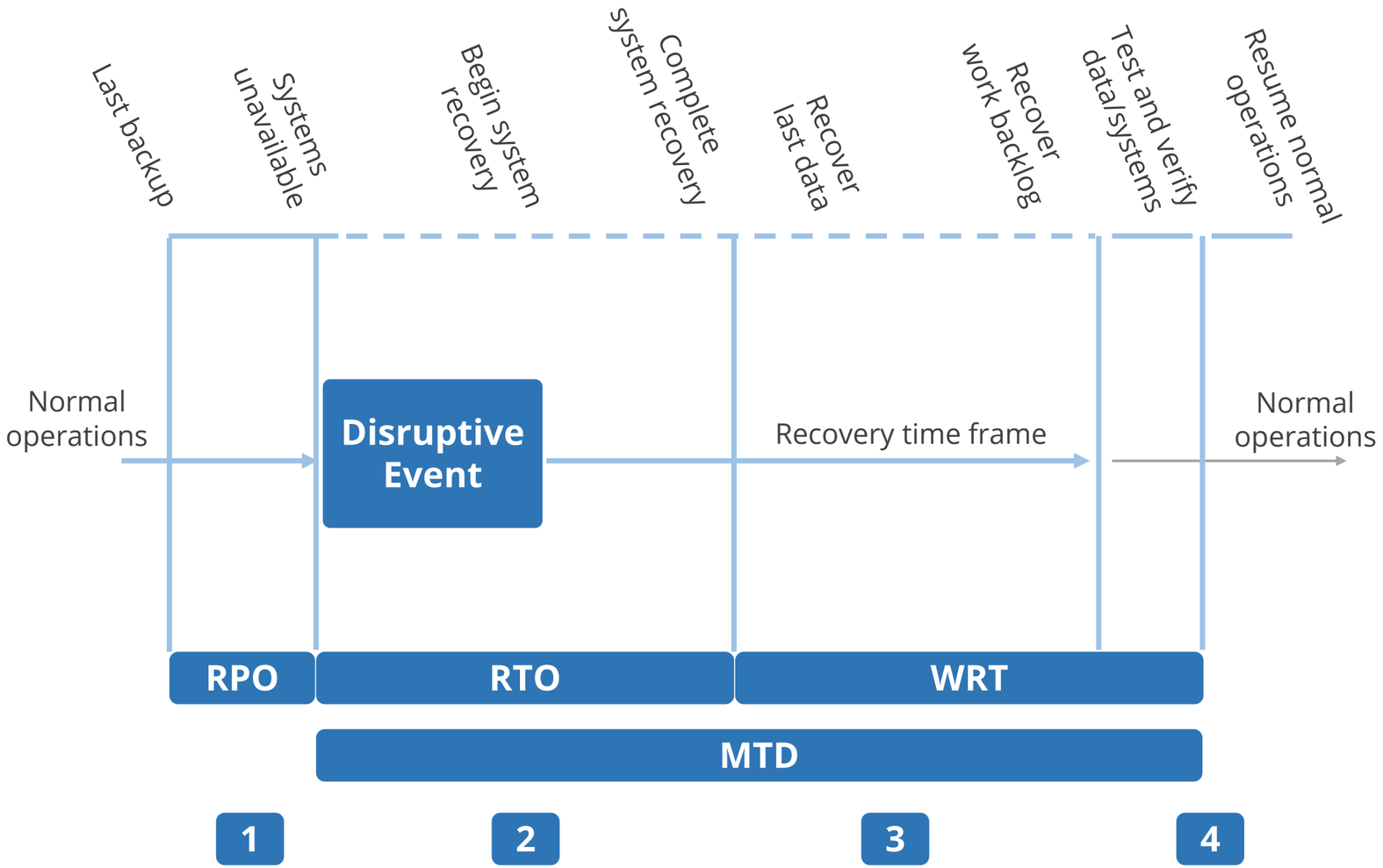
The BCP requires no service outage and permits up to one hour of data loss.

What is the RTO and RPO?

RTO is zero hour, and RPO is one hour.

Failure and Recovery

The various stages of failure and recovery are shown in the figure.



BCP or DRP Phase 3: Identify Preventive Controls

Preventive controls avert the potential impact of disruptive events.

The types of preventive controls include:

Existing controls	It is the process or device that mitigates the effect of a threat but cannot prevent the occurrence.
Physical controls	It refers to the fire suppression or sprinkler systems, access control systems, and security guards.
Procedural controls	It refers to the hiring and termination policies and clean desk policy.
Logical controls	It is the data storage protection and protection given to assets based on their location.

Quick Check

A business continuity team is analyzing to understand the potential effects of a disruption. Which of the following metrics is best used to determine the impact on critical business operations?

A. Residual risk

B. Total cost of ownership

C. Return on security investment

D. Priority of restoration

Overview of Personnel Security Controls

Managing Personnel Security

It implements measures to ensure that an organization’s employees are capable of meeting their security responsibilities.

Importance of Managing Personnel Security

The people inside the organization need access to data and resources to complete their assigned work and, therefore, have the potential to abuse these access privileges. It is important to:

- Protect sensitive information by securely managing the life cycle of employment
- Hire qualified and trustworthy individuals to reduce the risk to information assets
- Screen out individuals whose past actions indicate undesirable behavior to avoid potential risks to the organization

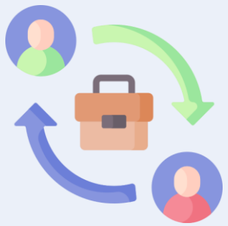
Personnel Management Controls

Job description

- Defines security needs related to personnel
- Defines the roles to which an employee needs to be assigned
- Defines the type and extent of access the position requires

Separation of duties

- Divides critical, significant, and sensitive work tasks among several individuals
- Helps protect against collusion
- Works as a preventive control



Job rotation

- Rotates employees among multiple job functions
- Provides knowledge redundancy
- Reduces risk of fraud, data modification, theft, and misuse

Personnel Management Controls

Cross-training

- Prepares employees for multiple job positions
- Helps with knowledge redundancy

Employee candidate screening

- Screens candidates based on criticality and sensitivity defined by the job description
- Completes before the candidate is onboarded into the organization

Non-disclosure agreement

- Protects confidential agreement within an organization

Personnel Management Controls

Non-compete agreement

- Legal contract that restricts an employee's ability to work for a competitor or start a competing business
- Protects company trade secrets and proprietary information

Mandatory vacation

- Administrative control that provides operational security by mandating employees to take vacations to identify any unethical activities

Employee termination process

- Takes place with at least one eyewitness
- Disables all access (logical or physical) of the terminated employee and escorts them out of office

Managing Personnel Security: Hiring Practices

Implementing these practices helps attract, select, and integrate the right candidates, ultimately enhancing the organization’s success and productivity.

- Perform background checks on education, prior employment, financial history, and criminal history
- Get the confidentiality agreements, such as non-disclosure agreement and intellectual property agreement, signed
- Get **Conflict of Interest Agreements** for the positions handling competitive information
- Get the **Non-Compete Agreements** for the positions in charge of unique corporate processes

Managing Personnel Security: Employee Termination

Employee termination policies include:

- **Voluntary:** Return of all access keys and badges, exit interview, and removal of system access
- **Involuntary:** Escort from premises, restriction of access immediately upon notification, and change of system passwords in the user's area

Managing Relationships

Controls for vendors, contractors, and consultants mostly act as preventive controls.

- Vendors and temporary employees should be given limited access to the information.
- Contractors should always be escorted within the organization.
- Consultants must be escorted whenever they visit your facility.

Acceptable Usage Policy (AUP)

It outlines the acceptable and unacceptable activities in the workplace and establishes employee expectations on how to use the company resources.

- Inappropriate use exposes the organization to risks including virus attacks, compromise of network systems and services, and legal issues.
- Employees should be aware of the consequence of noncompliance with their company's AUP.
- Employees should know that violation of this policy may be subject to disciplinary action, up to and including termination of employment.

What should an acceptable use policy contain?

- Introducing malicious programs
- Disclosing confidential information
- Sharing passwords
- Unauthorized security scanning
- Sending unsolicited email
- Circumventing security
- Making unauthorized representations

Privacy Policy Requirements

A privacy policy is a statement that discloses how a particular organization collects, stores, and utilizes the personal information provided by its users.

Any organization collecting any personal information from their customers, clients, or end users are legally required to publish a privacy policy on their site.

The exact content of a privacy policy will depend on the nature of the business, location of the business, location of the users, and the applicable laws.

At a minimum, an organization’s privacy policy should disclose what personal or sensitive information they collect, how they collected it, how they intend to use it, and whether they will disclose some or all the information to any third parties.

Quick Check

An organization is developing a new security policy, and the team is seeking approval. Why is it essential for senior management to endorse the security policy?

A. So that the management will accept ownership for security within the organization

B. So that employees will follow the policy directives

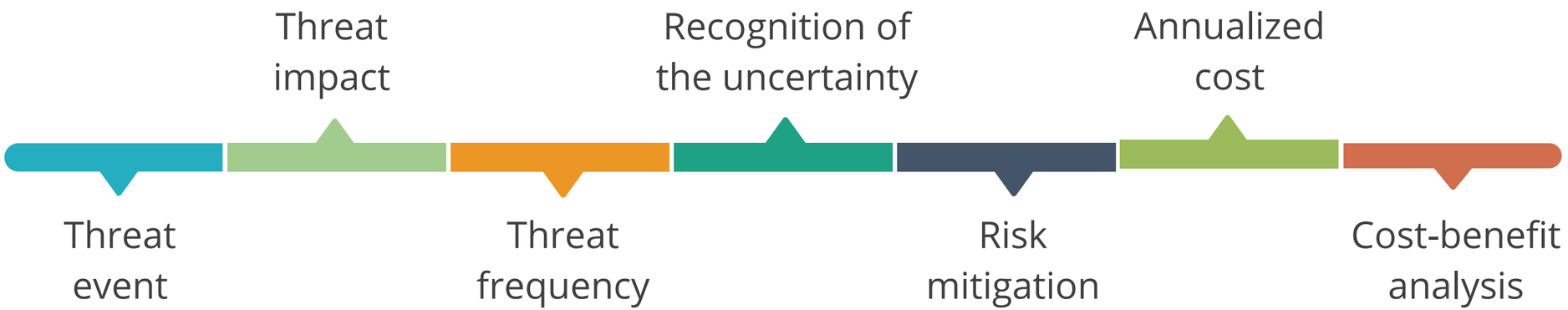
C. So that the management fulfills their due diligence requirements

D. So that external bodies will recognize the organization's commitment to security

Overview of Risk Management Concepts

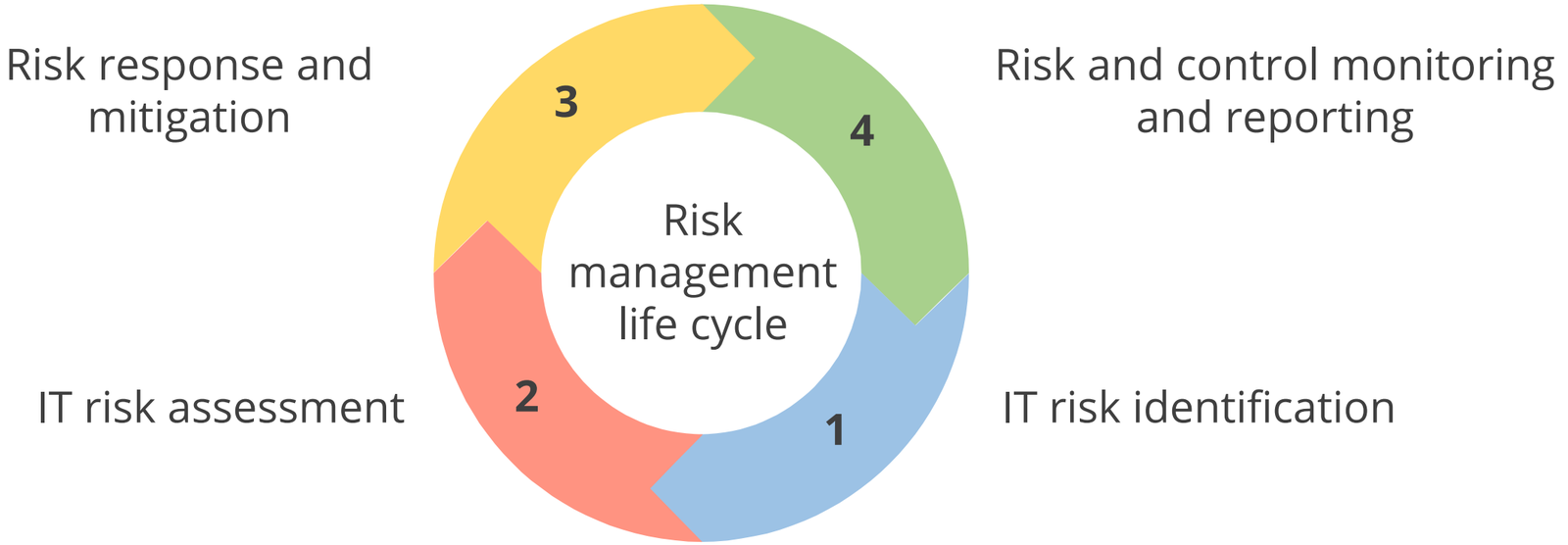
Risk Management

It is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain it at that level.



Risk Management: Steps

There are four steps in the risk management life cycle:



Risk Identification

It is the process of identifying any risks that could prevent an organization or program from reaching its objectives.

It helps companies understand and plan for potential risks.

It enables an organization to discover, categorize, and document risks.

Only identified risks can be evaluated and addressed with suitable responses, making this step crucial.

Risk Identification Method

Brainstorming

Interviews

Questionnaires

OEM updates

Regular testing

Subscriptions to blogs

Introduction to Risk Analysis

It is the analysis of the probability and consequences of each known risk.

- It prioritizes risks and calculates the cost of safeguards.
- It provides a cost-benefit comparison between the cost of safeguards and the cost of loss.
- It identifies and prioritizes the risk factors with great impact.
- It also integrates the security program objectives with the organization’s business objectives and requirements.

Goals of Risk Analysis

To identify organizational assets and their value

To identify vulnerabilities and threats

Goals of risk analysis

To balance the cost of countermeasure and the impact of threats

To measure probability and the impact of latent threats

Asset and Information Valuation

It involves assessing the value of an organization’s assets and information to prioritize security measures, manage risks, and ensure effective resource allocation.

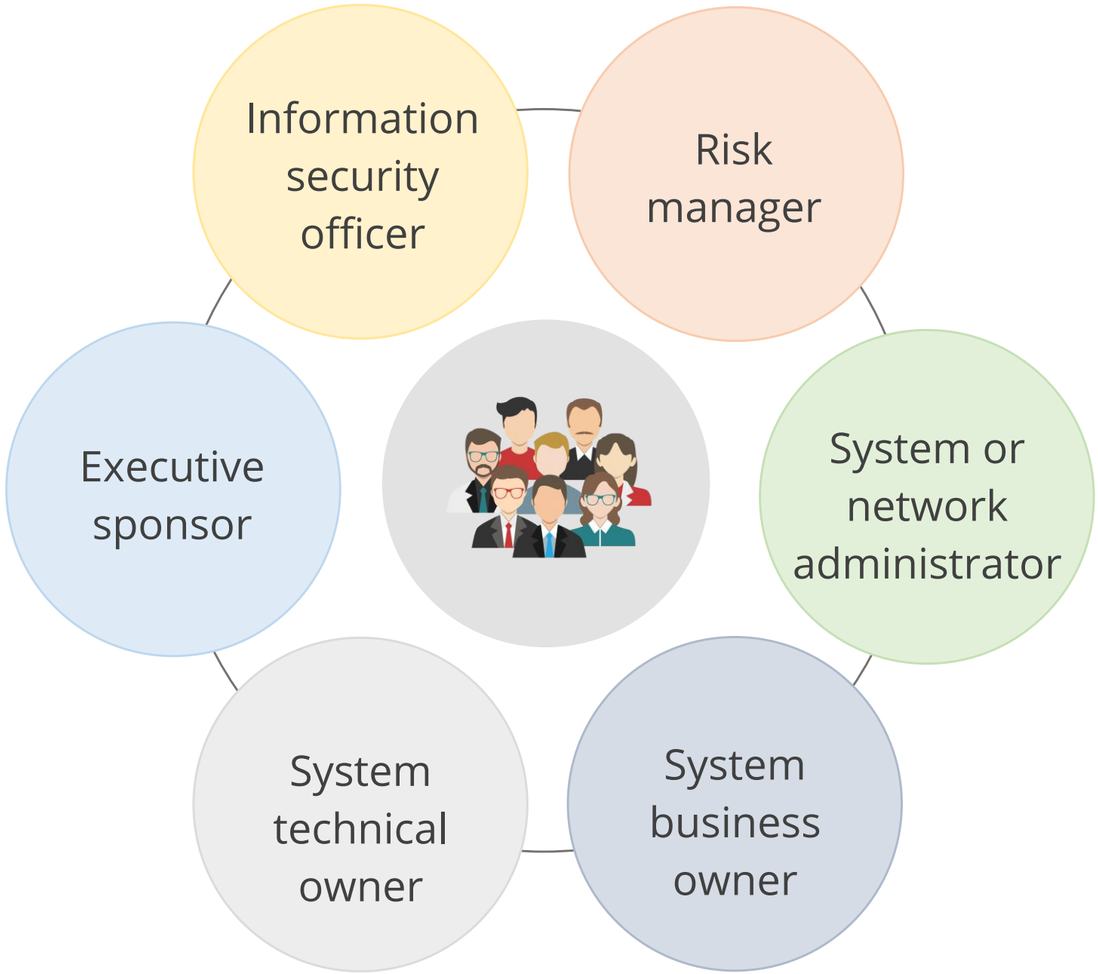
Asset and Information Valuation

The following issues should be considered when assigning values to an asset:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Value of intellectual property that went into developing the information
- Price others are willing to pay for the asset
- Cost to replace the asset if lost or damaged
- Operational and production activities that are affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization

Risk Analysis Team

An organization needs to form a risk analysis team to analyze risks effectively. These are the stakeholders in a risk analysis team:



Risk Analysis: Steps

It involves the following steps:

Risk analysis and assessment

Asset and information value assignment

Countermeasure selection and implementation

Types of Risk Analysis

There are two major types of approaches to risk analysis, and their features are as follows:

Quantitative Analysis

- Uses risk calculations that attempt to predict the level of monetary losses and the percentage of chance for each type of threat
- Objective in nature

Qualitative Analysis

- Situation and scenario-based
- Subjective in nature
- Does not assign numbers and monetary values to components and losses

Quantitative Risk Analysis

It provides a framework for organizations to quantify the potential impact of risks and make informed decisions based on data.

Key Terms in Quantitative Risk Analysis

Asset value (AV)	• Total value of assets
Exposure factor (EF)	• Percentage of loss the organization would suffer if a risk materializes • Also referred to as the loss potential
Single loss expectancy (SLE)	• Cost associated with a single-realized risk against a specific asset • SLE = AV * EF • Calculated in dollars

Key Terms in Quantitative Risk Analysis

Annualized rate of occurrence (ARO)

- Frequency with which a specific threat occurs within a single year
- Ranges from 0 (threat will not occur) to large numbers
- Also known as probability determination

Annualized loss expectancy (ALE)

- Possible yearly cost of all instances of a specific threat realized against a specific asset
- ALE = SLE * ARO

Annual cost of safeguard (ACS)

- Cost associated in procuring, developing, and maintaining control against a potential threat
- Should not exceed the ALE

Quantitative Risk Analysis: Steps

Step 1: Assign asset value

Step 2: Calculate exposure factor

Step 3: Calculate single loss expectancy

Step 4: Assess annualized rate of occurrence

Step 5: Derive annualized loss expectancy

Step 6: Perform cost-benefit analysis of countermeasure

Quantitative Risk Analysis: Problem

Problem

Fire destroys a server with encrypted data.

Consider the following conditions:

- Asset value = $6,000
- EF = 50%
- ARO = 10% chances of fire in one year

Solution

- Single Loss Expectancy (SLE) = $6,000 x 50% = $3,000
- Annual Loss Expectancy (ALE) = 10% x $3,000 = $300

Qualitative Risk Analysis

Qualitative analysis techniques include judgment, best practices, intuition, and experience. Some of the qualitative techniques used to gather data include:

- Delphi
- Brainstorming
- Storyboarding
- Focus groups
- Surveys
- Questionnaires
- Checklists
- One-on-one meetings
- Interviews

Qualitative Risk Analysis

The following table deals with some of the threats, the level of threat, and countermeasures:

Threat	Threat probability	Impact	Countermeasure
Fire	Low	High	Fire extinguishers
Theft	Medium	High	Key cards and guards
Logical intrusion	Medium	High	Intrusion prevention system

Qualitative Risk Analysis

The type of approach to risk analysis will be decided based on the risk analysis team, management, risk analysis tools, and culture of the company.

The chart below sorts different attributes into qualitative and quantitative risk analysis.

Attributes	Quantitative	Qualitative
Requires complex calculations	√	X
Requires high degree of guess work	X	√
Provides credible cost/benefit analysis	√	X
Provides opinions of the individuals who know the process well	X	√
Shows clear-cut losses that can be accrued within one year	√	X

Hybrid Analysis

It uses both quantitative and qualitative analysis.
The following are some points about why hybrid analysis is required:

- It is almost impossible to carry out only quantitative assessment.
- Qualitative analysis does not provide sufficient data to make financial decisions.
- Quantitative evaluation is used for financial values of tangible assets.
- Qualitative assessment can be used for priority values of intangible assets.

Cost-Benefit Analysis

It is a critical component of risk management that involves evaluating the potential costs associated with a risk against the benefits of implementing a countermeasure.

By comparing the two, organizations can make informed decisions about which risks to prioritize and how to allocate resources for mitigation.

Cost-Benefit Analysis: Problem

A commonly used cost-benefit calculation for a given safeguard:

Value of the safeguard to the company = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (Annual cost of safeguard)

Problem

- ALE of the threat of a fire bringing down a web server prior to implementing the suggested safeguard = $10,000
- ALE after implementing the safeguard= $2,000
- Annual cost of maintenance and operation of the safeguard = $500

Solution

- Value of the safeguard to the company = $10,000 - $2,000 - $500
  = $7,500

Countermeasure Selection: Other Factors

Some of the factors that influence the selection of countermeasures or safeguards:

Total Cost of Ownership (TCO)	It is the total cost of a mitigating safeguard.
Return on Investment (ROI)	It is the amount of money saved by implementing a safeguard.
Uncertainty	It refers to the degree of lack confidence in an estimate. This is expressed as a percentage, from 0 to 100 percent. For example, a 25 percent confidence level in something indicates a 75 percent uncertainty level.

Risk Response

Responding to risk involves the following:

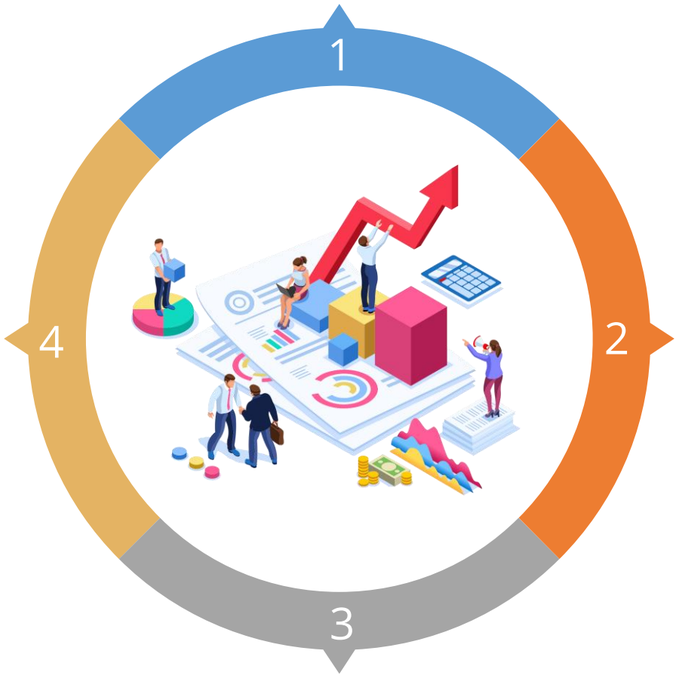
Evaluating countermeasures, safeguards, and security controls using a cost-benefit analysis

Providing a proposal of response options in a report to the senior management

Adjusting findings based on other conditions, concerns, priorities, and resources

Handling Risk

Risk treatment can be done in the following four ways:



Risk Mitigation

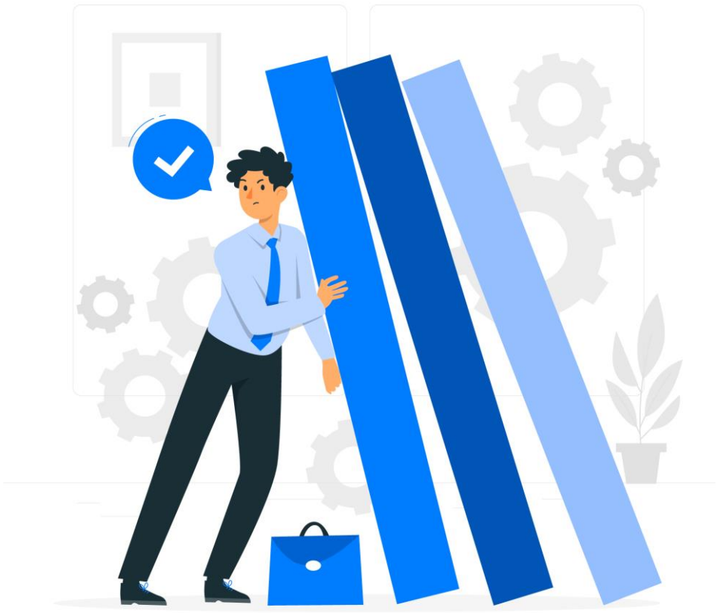
It involves implementing safeguards and countermeasures to eliminate vulnerabilities or block threats.

Examples

- Implementing intrusion prevention systems (IPS) and data loss prevention (DLP)
- Implementing a web application firewall (WAF) to address the shortcomings of a network firewall in handling web application attacks

Risk Avoidance

It involves terminating the associated activity that introduces the risk.

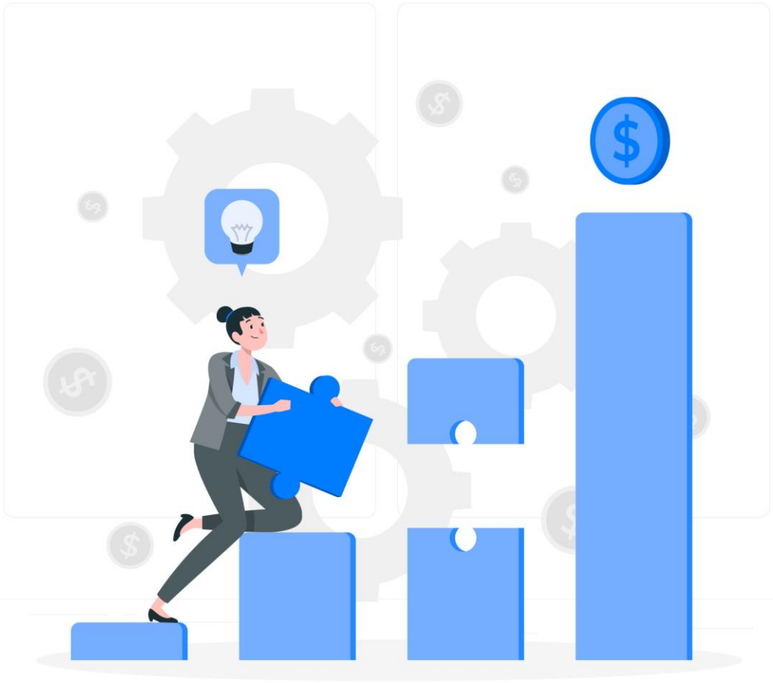


Examples

- Not buying a property or business to avoid taking on the liability that comes with it
- Not flying to avoid the risk of the airplane being hijacked

Risk Transfer

It involves shifting the cost of loss a risk represents onto another entity or organization.



Examples

- **Cyber Insurance:** Purchasing insurance to cover potential cyber-related losses
- **Outsourcing:** Contracting out certain business functions to third-party organizations, transferring the associated risks

Risk Acceptance

It occurs when the cost-benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value.

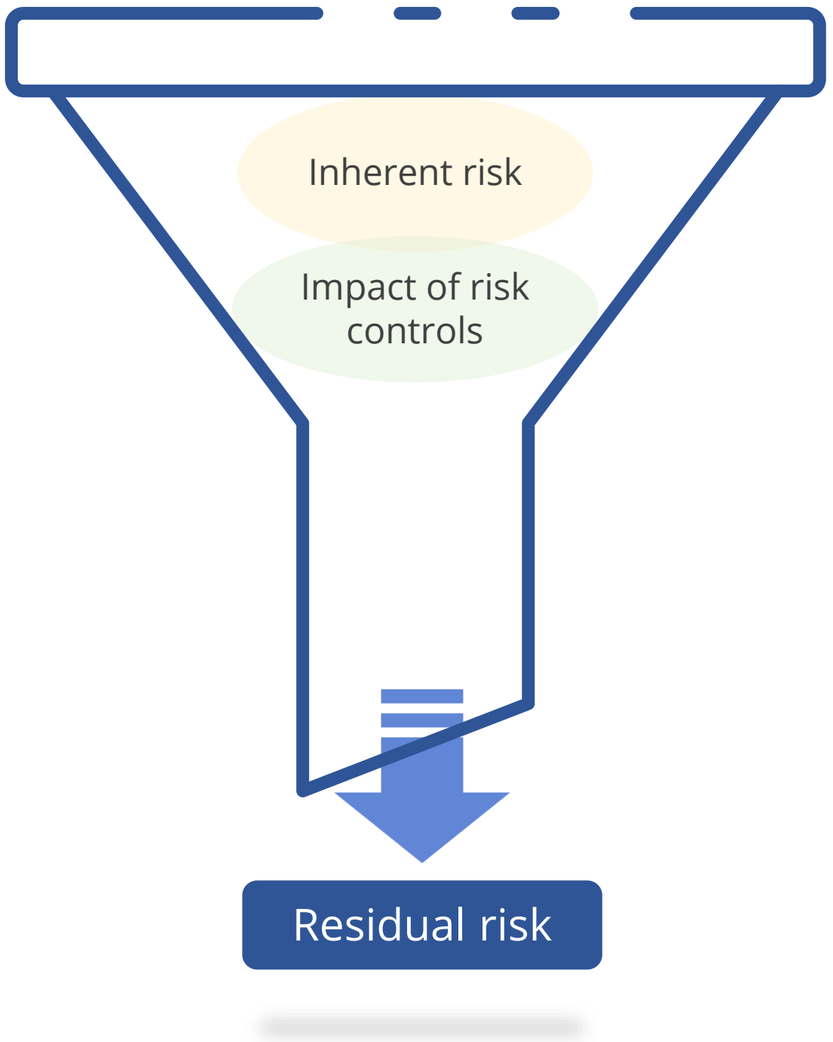
Examples

- When the cost of the asset is less than the cost of the countermeasure
- When there are changes in government policies
- When the client changes their policies

This strategy involves recognizing the risk and deciding not to take any action to mitigate it.

Residual Risk

It is the risk that remains after countermeasures and controls have been implemented.

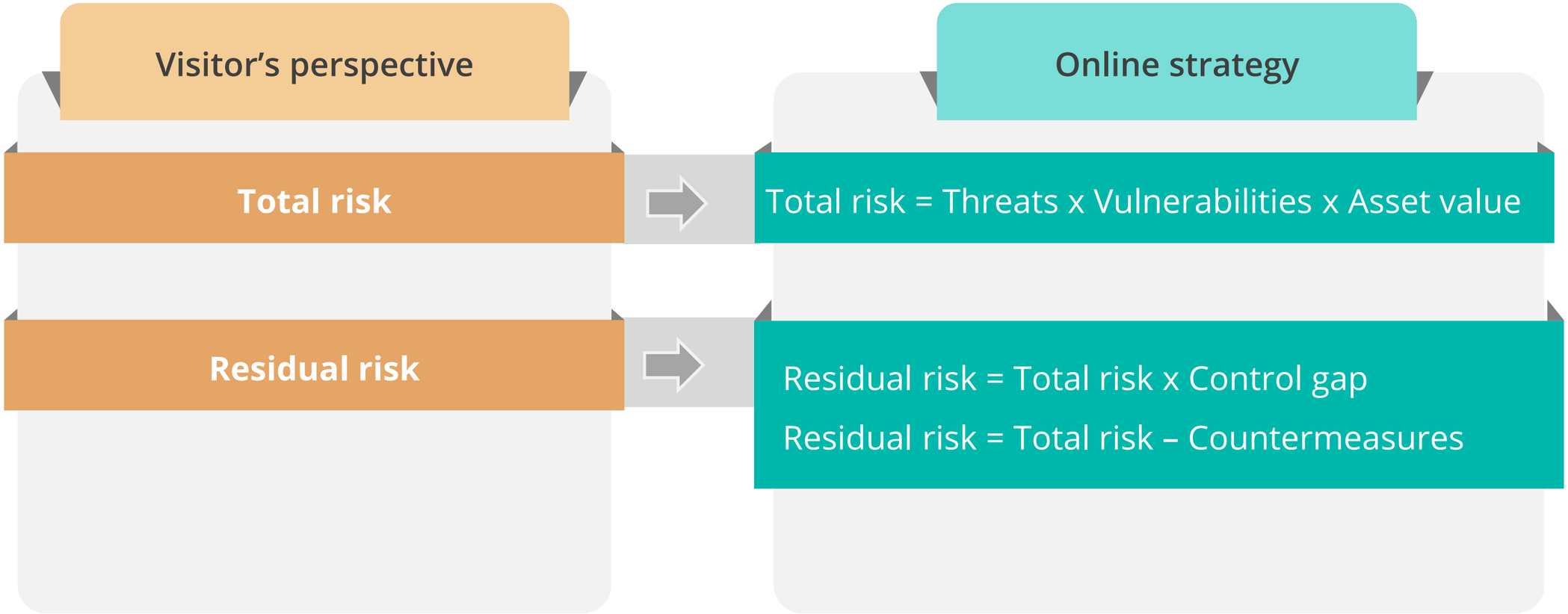


Examples

It acknowledges that it is not always possible to eliminate the risks entirely.

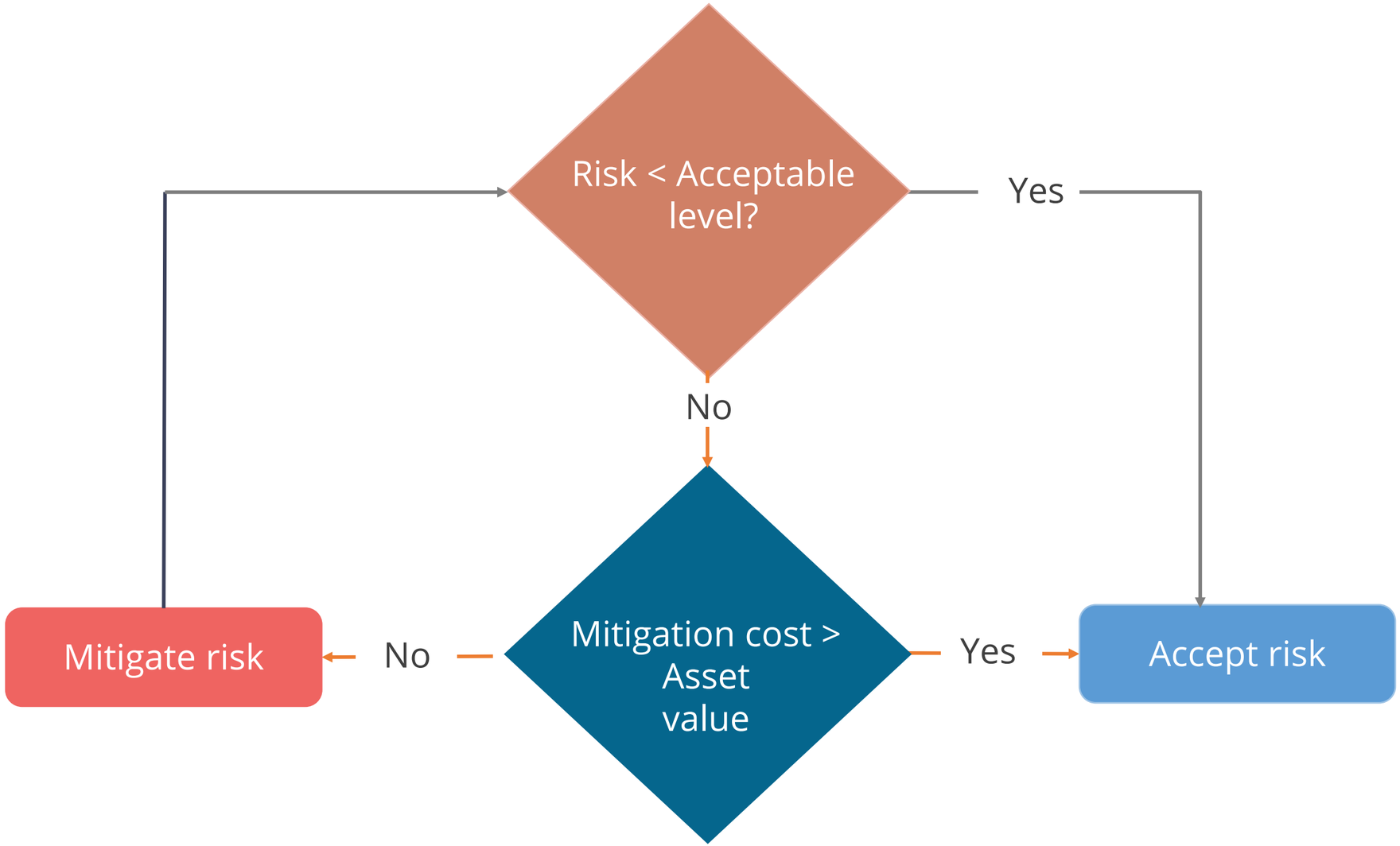
Risk Calculation

Conceptual formulas to calculate total risk and residual risk:



Residual Risk Mitigation

Here is a flowchart that explains the steps in the risk mitigation process:



Risk Capacity, Risk Appetite, and Risk Tolerance

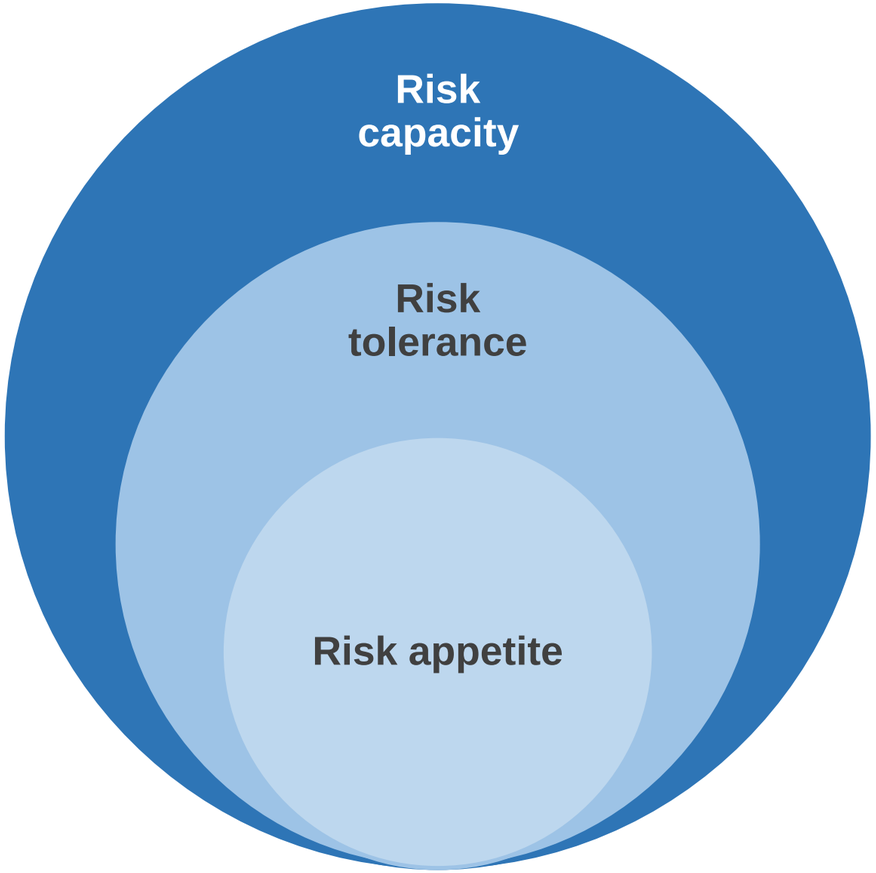
Risk capacity	It is the maximum risk an organization can afford to take.
Risk appetite	It is the amount of risk that an organization is willing to take.
Risk tolerance	It is the acceptable level of deviations from the risk appetite.

Risk Capacity, Risk Appetite, and Risk Tolerance

Risk capacity is always greater compared to tolerance and appetite.

Risk tolerance can either be equal to or greater than appetite.

Risk appetite generally should be within the risk appetite of the organization. In no case should it exceed the risk capacity.



Aggregated Risk And Cascading Risk

Aggregated risk

- It is a significant impact caused by a large number of minor vulnerabilities.
- These minor vulnerabilities would not have any major impact individually. However, when exploited at the same time, they can cause a huge impact.

Cascading risk

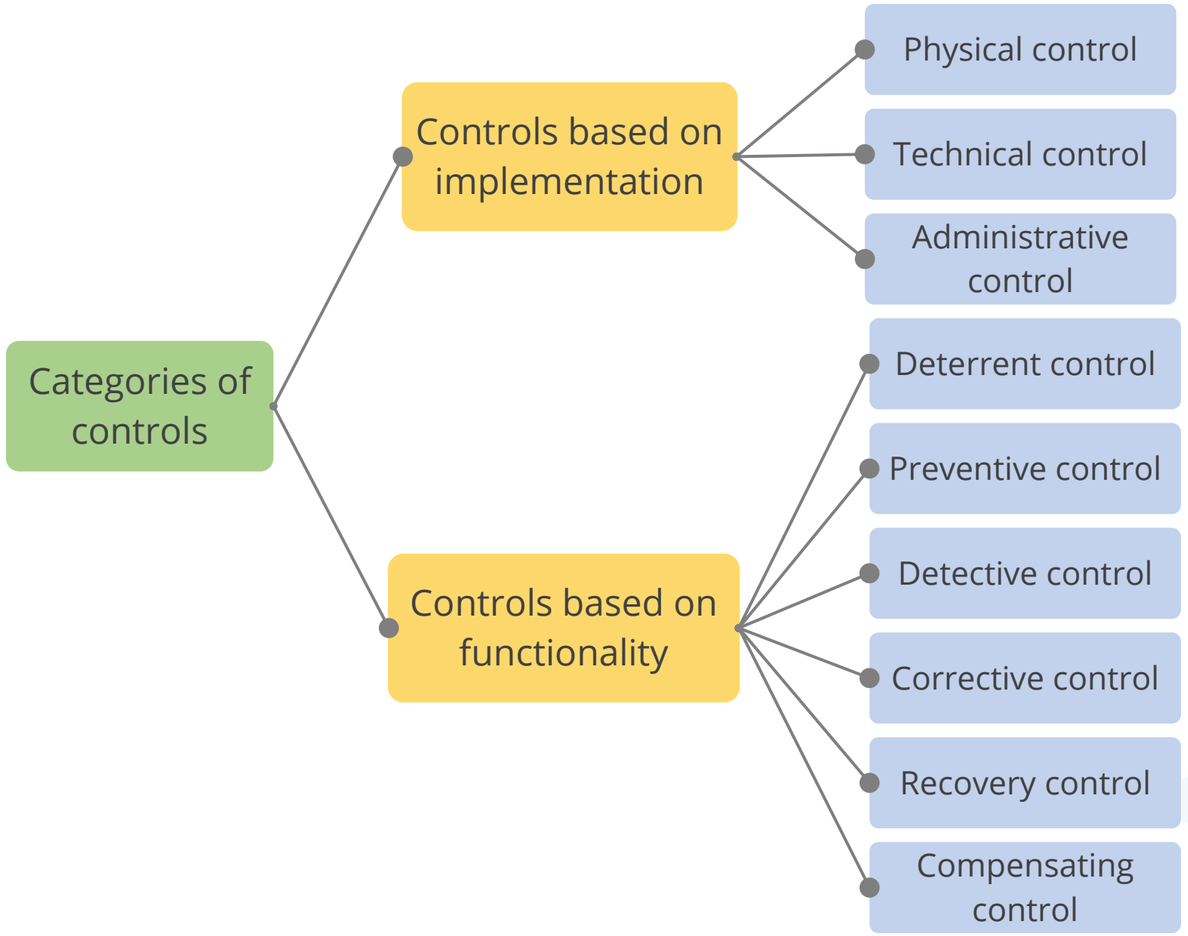
- It happens when one failure leads to a chain reaction of failures and is more relevant where IT operations have close dependencies.
- The security manager should consider the impact of the failure of one activity on other dependent systems.

Controls or Countermeasures

Security controls are the measures taken to safeguard an information system from attacks against the confidentiality, integrity, and availability of the information system.

Security controls are selected and applied based on a risk assessment of the information system.

The risk assessment process identifies system threats and vulnerabilities, and then, security controls are selected to reduce or mitigate the risk.



Controls Based on Implementation

There are three types of controls based on implementation:

Administrative controls

- Also known as soft controls as they are more management-oriented

Examples

Security documentation, risk management, personnel security, and training

Technical controls

- Also called logical controls and are the software or hardware components

Examples

Firewalls, IDS, encryption, identification, and authentication mechanisms

Physical controls

- Items put into place to protect a facility, personnel, and resources

Examples

Security guards, locks, and fencing

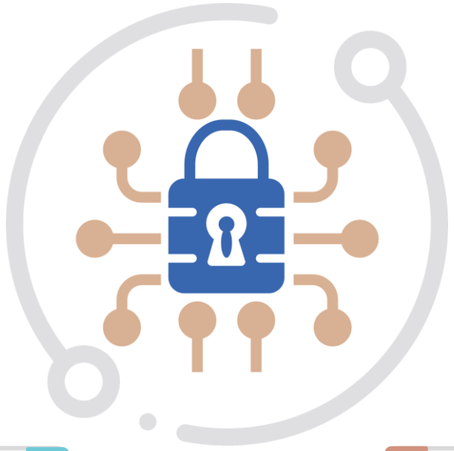
Controls Based on Functionality

The six controls based on functionality are:

Deterrent	Intends to discourage a potential attacker
Preventive	Intends to avoid an incident from occurring
Corrective	Fixes components or systems after an incident has occurred
Recovery	Intends to bring the environment back to regular operations
Detective	Helps identify an incident’s activities and potentially an intruder
Compensating	Provides an alternative measure of control

Security Control Assessment (SCA)

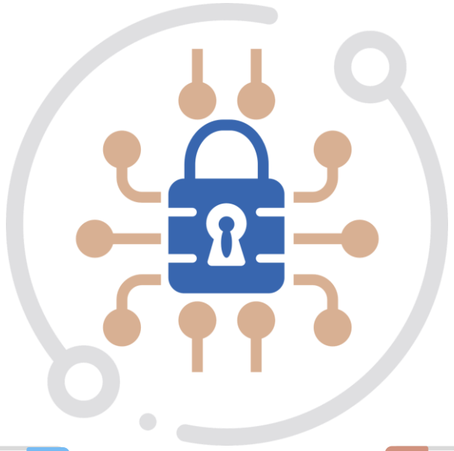
It evaluates the effectiveness of security measures in protecting an organization's information assets by identifying, assessing, and testing them to mitigate identified risks.



It is a comprehensive evaluation or assessment of the management, operational, and technical security controls of an information system.

Its goal is to determine the extent to which the controls are meeting the security requirements of the system.

Security Control Assessment (SCA)

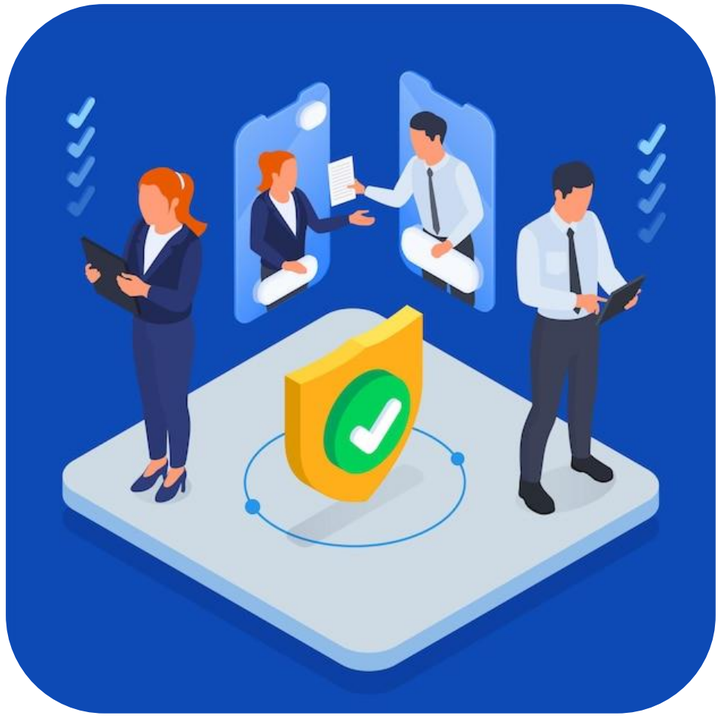


The types of system tests conducted include audits, security reviews, vulnerability scanning, and penetration testing.

Security control assessments are conducted before the system is put into production and annually thereafter.

Security Control Assessment (SCA)

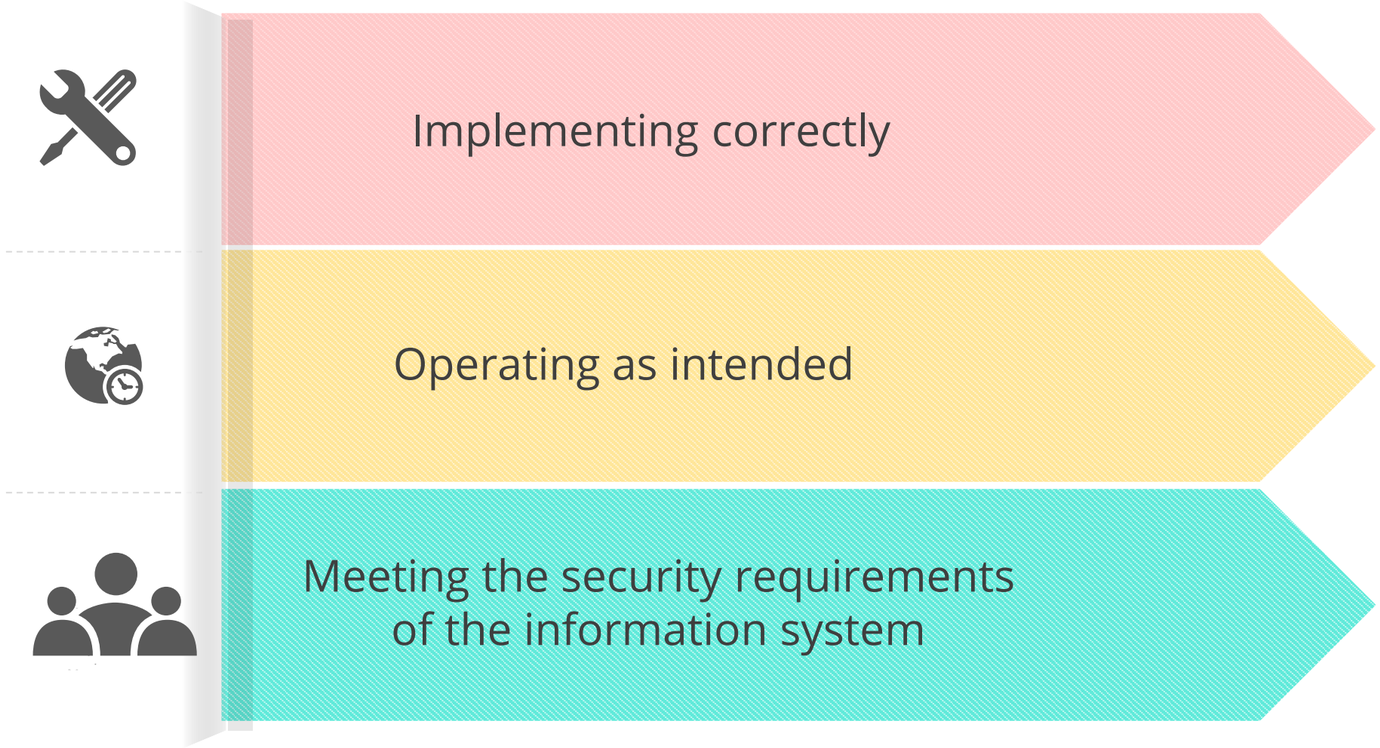
The results of an SCA provide:



- Evidence of the effectiveness of implemented controls
- An indication of the quality of the risk management processes employed within the organization
- Information about the strengths and weaknesses of information systems that are supporting organizational missions and business functions

Assurance for Security Control Effectiveness

To ensure security control effectiveness, one should compile evidence that the controls are:



Security Control Assessment Team

The SCA team is an individual, group, or organization responsible for conducting a comprehensive security control assessment of an information system.

- They may also provide a risk assessment of the severity of weaknesses or deficiencies discovered in the information system and recommend corrective actions to address the identified vulnerabilities in the system.
- They prepare the final security assessment report containing the results and findings of the assessment.

Note:

Common controls utilized for high and moderate impact systems must be performed by an independent assessment team.

Risk Monitoring and Measurement

The risk environment is dynamic because the organization’s internal and external environments are constantly changing.

Organizations should continuously monitor the IT risks and controls to ensure the efficiency and effectiveness of the IT risk management strategy and its alignment with business objectives.

Risk Register

It is a centralized repository that records identified risks, their characteristics, and their management plans.

It is a crucial document in risk management processes that provides a detailed log of risks identified during a risk assessment.

It is a critical risk management tool that provides a structured way to track and evaluate risks over time.

It includes key risk indicators (KRIs), identifies risk owners, and specifies the risk threshold, helping organizations monitor and manage risks effectively

Components of Risk Registers

Risk ID

KRIs

Description

Risk owners

Current status

Risk thresholds

Sample Risk Register

Risk ID	Description	Indicator	Owner	Threshold	Status	Plan
1	Data breach	Financial loss	IT Dept	$10,000	Under threshold	Implement 2FA
2	Non compliance	Legal penalties	Legal Dept	2 incidents	Over threshold	Review compliance policy
3	Supply chain disruption	Operational delay	Ops Dept	5 days	Under threshold	Diversify suppliers
4	Reputational damage	Customer churn	Marketing	10%	Under threshold	Crisis communication plan

Reporting Significant Changes

Risk assessments should be done at regular intervals to address emerging risks and understand trends in the risk factor.

A security manager should present the status of the organization's updated risk profile to management at regular intervals.

Management should also be updated about any significant events or incidents impacting the organization.

Risk Communication

It is key to the effective implementation of the risk management strategy.

Communication should involve all relevant stakeholders, and communication channels should enable interaction in both directions.

Risk Measurement

KRIs and KPIs can be used to measure, monitor, and report risk.

Key risk indicator (KRI)

- It is a measure used in risk management to indicate how risky an activity is.
- By comparing an appropriate set of KRIs with defined thresholds, organizations receive an early warning when a risk approaches an unacceptable level.

Key performance indicators (KPIs)

- They are used to measure how well a process is performing in terms of its stated goal.
- They are used to set benchmarks for risk management goals and to monitor whether those goals are being met.

Risk Reporting

A risk report includes information on current risk management capabilities and actual status and trends about risk.

Results of the risk monitoring process need to be documented and reported to the senior management on a regular basis.

A significant security incident or significant changes in risk should trigger a report to the senior management and a reassessment of the risk controls.

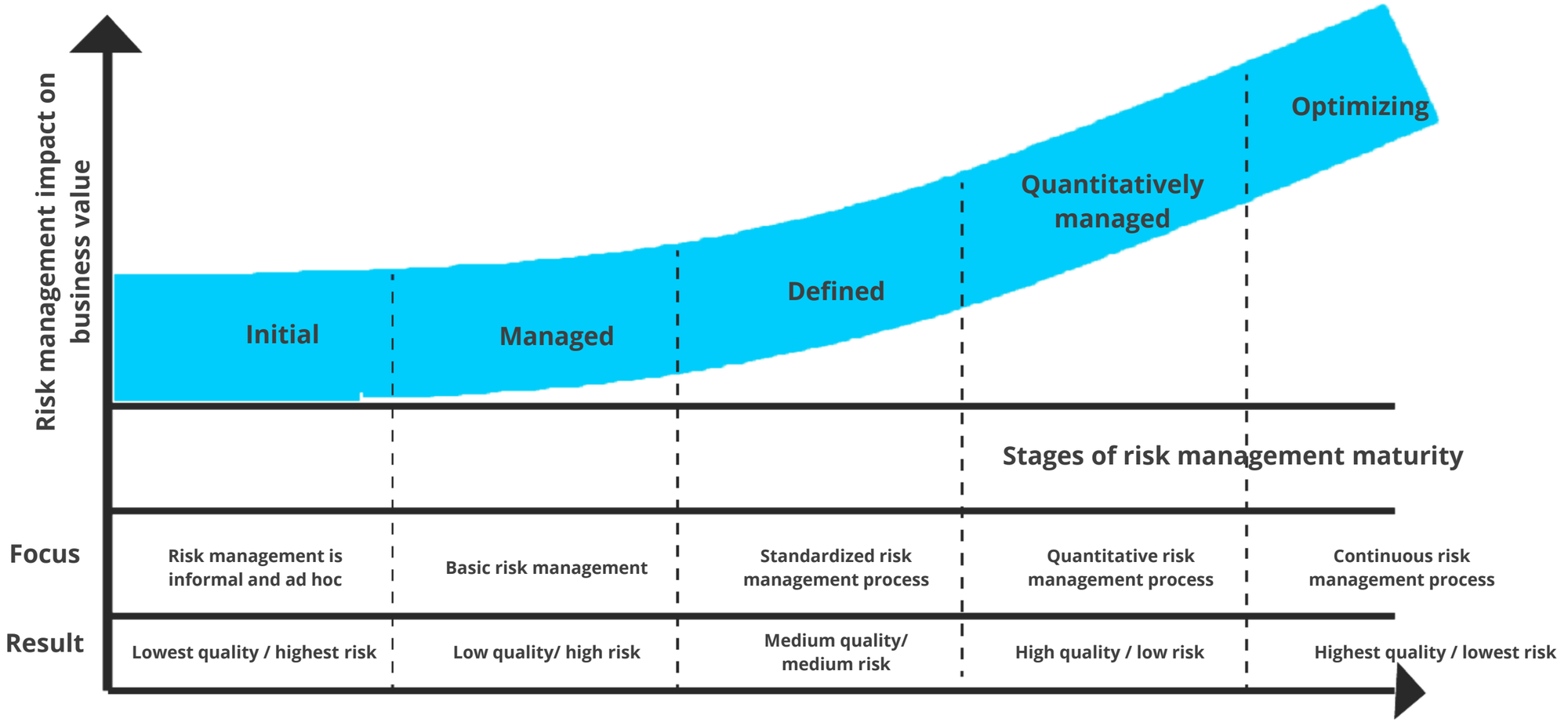
Continuous Improvement

A risk maturity model helps organizations improve their risk management processes by identifying their capabilities.

A mature risk management program helps prevent, detect, and respond to security incidents.

Maturity and growth comes from practice and learning from past experiences.

Continuous Improvement



Risk Frameworks

They are used to identify, measure, manage, monitor, and report significant risks to the achievement of business objectives.

There are three risk frameworks, namely:

- NIST Risk Management Framework
- ISO 31000
- ENISA Risk Management or Risk Assessment (RM/RA) Framework

Quick Check

While conducting a risk assessment, the security team is prioritizing various factors. What is the most important consideration during this process?

A. Assets have been identified and appropriately valued.

B. Appropriate risk response has been identified.

C. Single loss expectancy has been calculated.

D. Priority of restoration is maintained.

Understand and Apply Threat Modeling Concepts and Methodologies

Threat Modeling

It is a security process where potential threats in a system are identified, quantified, and addressed.

It can be performed as a proactive measure during the planning and design phase of the SDLC and is continued throughout the life cycle.

A reactive approach to threat modeling takes place after a product has been created and deployed.

Threat Modeling

Goals of threat modeling

- Reducing the number of security-related coding and design defects
- Reducing the severity of remaining defects

Threat Modeling

Approaches to threat modeling:

Proactive approach

- Also known as the defensive approach
- Takes place during early stages of systems development
- Based on predicting threats and design-specific countermeasures during the coding and crafting process

Reactive approach

- Also known as the adversarial approach
- Takes place after a product has been created and deployed
- Core concept behind ethical hacking, PT, source code review, and fuzz testing

Threat Modeling Steps

Identifying threats

- Focused on assets
- Focused on attackers
- Focused on software

Categorizing threats

- STRIDE model

Determining and diagramming potential attacks

- Data flow diagrams
- Privilege boundaries
- Elements

Performing reduction analysis

- Trust boundaries
- Data flow path
- Input points
- Privilege operation
- Security stance and approach

Prioritizing and responding

- DREAD model

Step 1: Identification of Threats

Focused on attackers

- Frames the threats based on the mindset of the perceived attacker
- Determines and addresses the attacker's characteristics, skill sets, motivations, and intentions

Focused on assets

- Identifies the elements of the system that have risk associated with them
- Classifies assets according to their intrinsic value to a potential attacker

Focused on system or software

- Establishes a system structure first and then identifies relevant attack vectors on the macro- and micro-levels of interaction between subsystems

Step 2: Categorization of Threats (STRIDE Approach)

Spoofing	Gaining access to a target system through the use of a falsified identity
Tampering	Falsifying communications or altering static information
Repudiation	Denying having performed an action or activity
Information disclosure	Revealing or distributing private, confidential, or controlled information to external or unauthorized entities
Denial of service (DoS)	Preventing an authorized use of a resource
Elevation of privilege	Transforming a limited user account into an account with greater privileges, powers, and access

Step 3: Determining and Diagramming Potential Attacks

Once the threats are identified, the next step is to determine the potential attack concepts that could materialize.

It is often accomplished by data flow diagrams, privilege boundaries, and the elements involved.

Once a diagram has been crafted, all the involved technologies are identified.

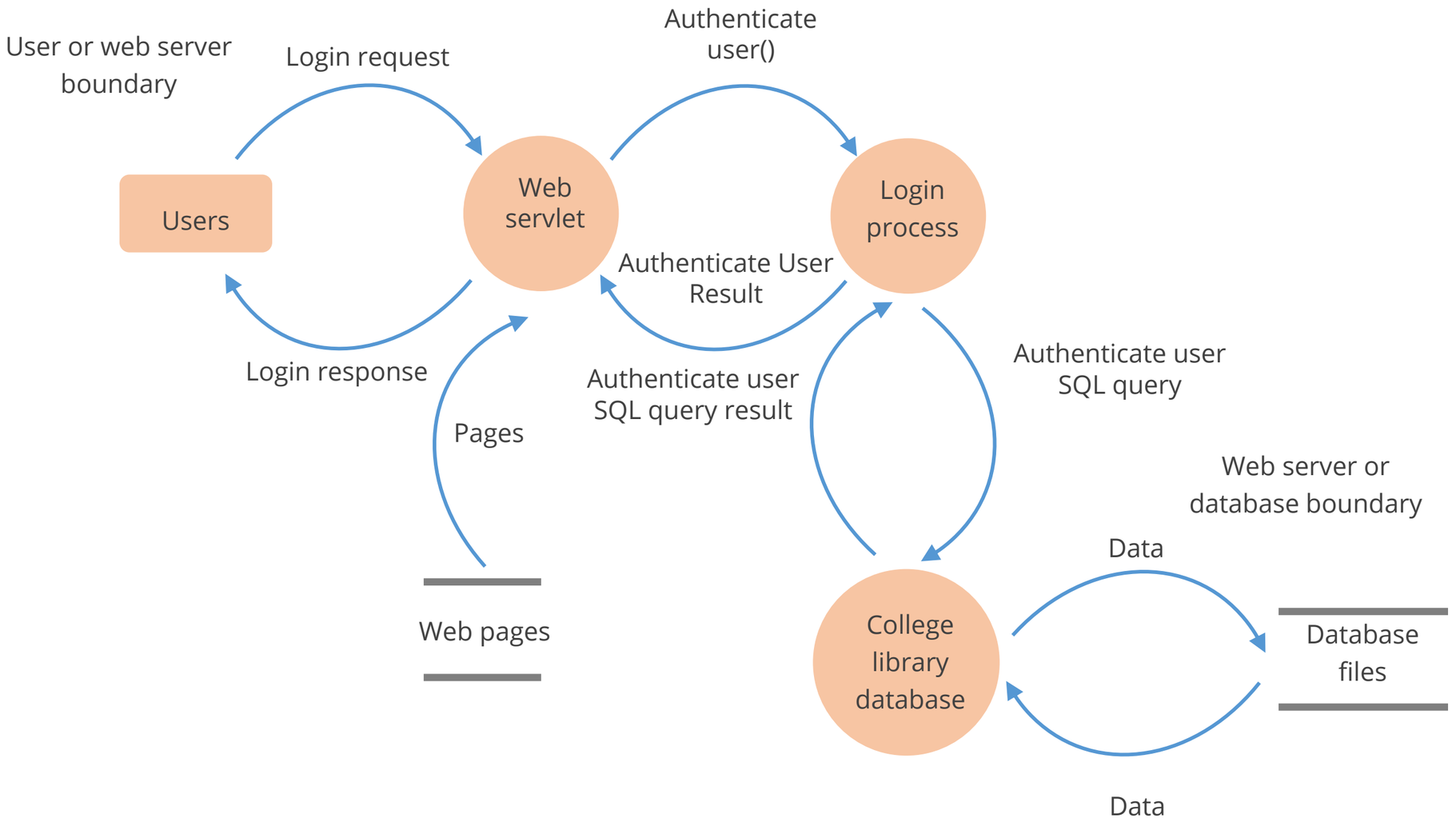
Attacks that could be targeted at each element of the diagram are identified.

Note:

Attacks should include all forms: logical, physical, and social.

Step 3: Determining and Diagramming Potential Attacks

The given diagram shows the privilege boundaries and the elements involved:



Step 4: Performing Reduction Analysis

It involves decomposing the application, system, or environment.

Input points

Data flow paths

Privilege operations

Trust boundaries

Security stance and approach

Step 5: Prioritization and Response

This step involves rating the threats to prioritize and address the most significant threats first.

Risk posed by a particular threat is equal to the probability of the threat occurring against the potential damage.

Risk = Probability * Potential damage

If a threat is rated as high, it poses a significant risk and needs to be addressed as soon as possible.

Medium threats need to be addressed but with less urgency.

Low-level threats can be ignored depending upon the effort and cost required to address these.

Step 5: Prioritization and Response

The DREAD rating system is a risk assessment framework used to evaluate the severity of threats and vulnerabilities.

Damage potential	How severe is the damage likely to be if the threat is realized?
Reproducibility	How complicated is it for attackers to reproduce the exploit?
Exploitability	How hard is it to perform the attack?
Affected users	How many users are likely to be affected by the attack?
Discoverability	How hard is it for an attacker to discover the weakness?

DREAD Rating

Threat description	D	R	E	A	D	Total	Rating
An attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
Injection of SQL commands	3	3	3	3	2	14	High

Threat Template

It is a structured document that outlines potential security threats to a system, along with key details

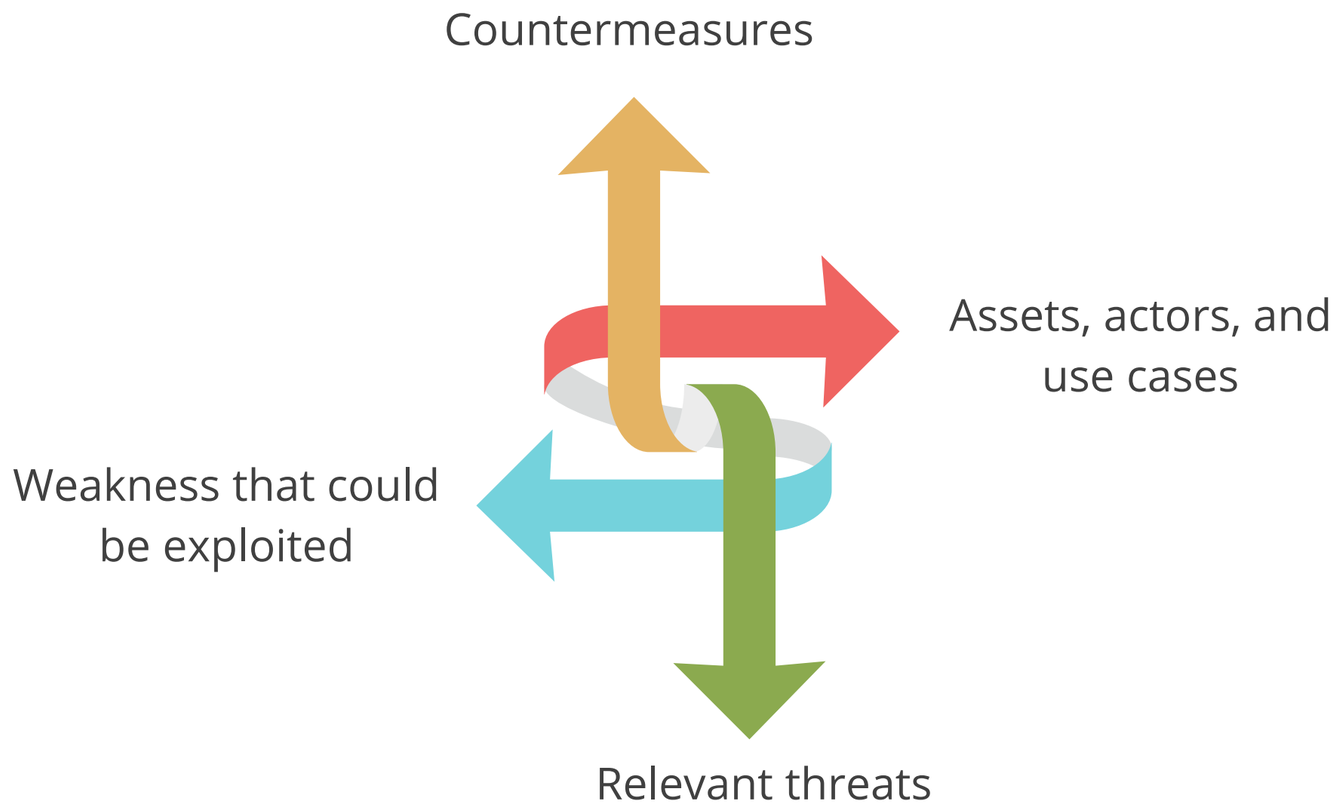
Threat description	Injection of SQL commands
Threat target	Data access component
Risk rating	-
Attack techniques	An attacker appends SQL commands to username, which is used to form an SQL query.
Countermeasures	Use a regular expression to validate the username and use a stored procedure that uses parameters to access the database

Threat Template

Threat description	Attacker obtains authentication credentials by monitoring the network
Threat target	User authentication process in a web application
Risk rating	High
Attack techniques	An attacker uses a network monitoring software.
Countermeasures	Use SSL to provide an encrypted channel

Threat Modeling Outcomes

Outcome of a threat modeling activity is a threat module document that identifies:

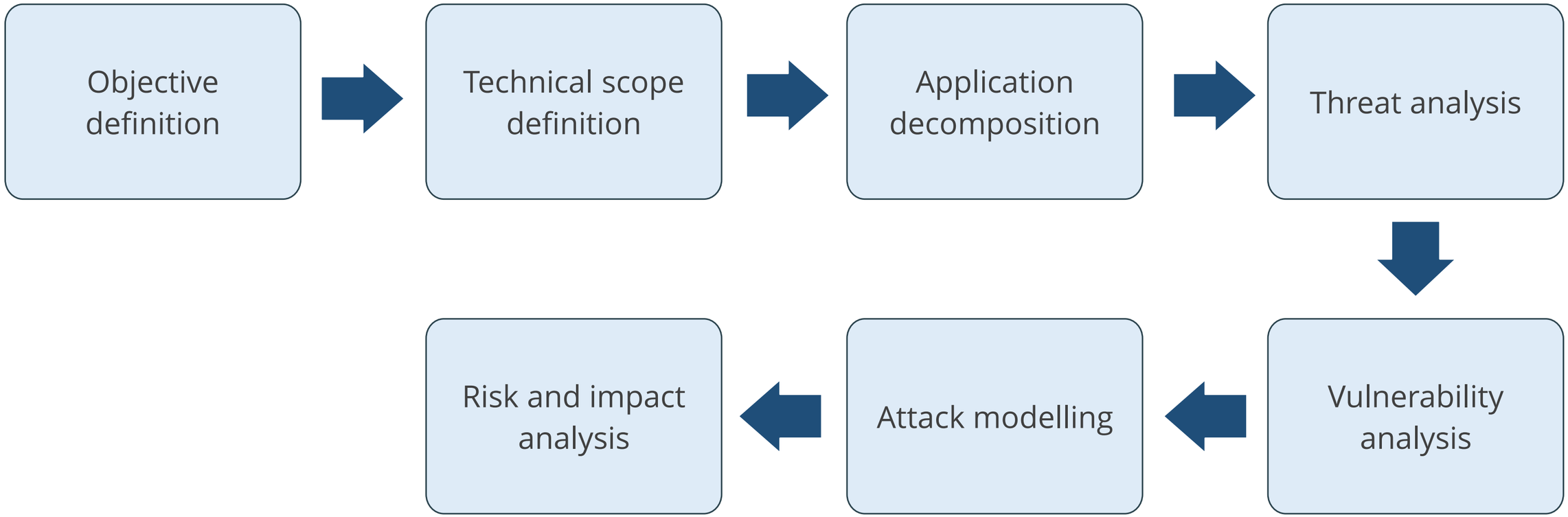


PASTA

It stands for **Process for Attack Simulation and Threat Analysis** and outlines the seven steps for risk-based threat analysis.

It integrates security and business objectives in threat modeling and allows security teams to leverage existing work such as business impact analysis (BIA).

PASTA: Steps


Objective definition
Technical scope definition
Application decomposition
Threat analysis
Vulnerability analysis
Attack modelling
Risk and impact analysis

Quick Check

During a security workshop, a team is using the STRIDE model to assess threats to their applications. Which of the following is NOT an element of the STRIDE threat model?

A. Spoofing

B. Elevation of privilege

C. Repudiation

D. Disclosure

Overview of Supply Chain Risk Management (SCRM) Concepts

Supply Chain

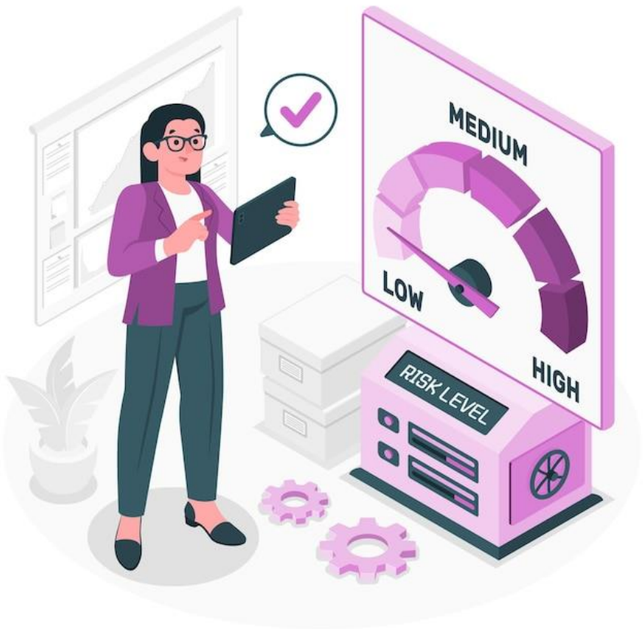
It is the network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product.

It starts with the delivery of source materials from the supplier to the manufacturer, eventually delivering to the end user.

A supply chain compromise is an occurrence within the supply chain where an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits.

Supply-Chain Risk Management (SCRM)

It is a process to help identify, monitor, detect, and mitigate threats to supply chain continuity and profitability.



A security chain compromise can occur anywhere within the system development life cycle of the product or service.

Risks Associated with Hardware, Software, and Services

Here are a few risks associated with hardware, software, and services:

Counterfeit hardware or hardware with embedded malware

Poor information security practices by lower-tier suppliers

Software security vulnerabilities in supply chain management or supplier systems

Compromised software or hardware purchased from suppliers

Mitigating Risks Associated with Hardware, Software, and Services

These supply-chain risks can be mitigated during acquisition life cycle by:

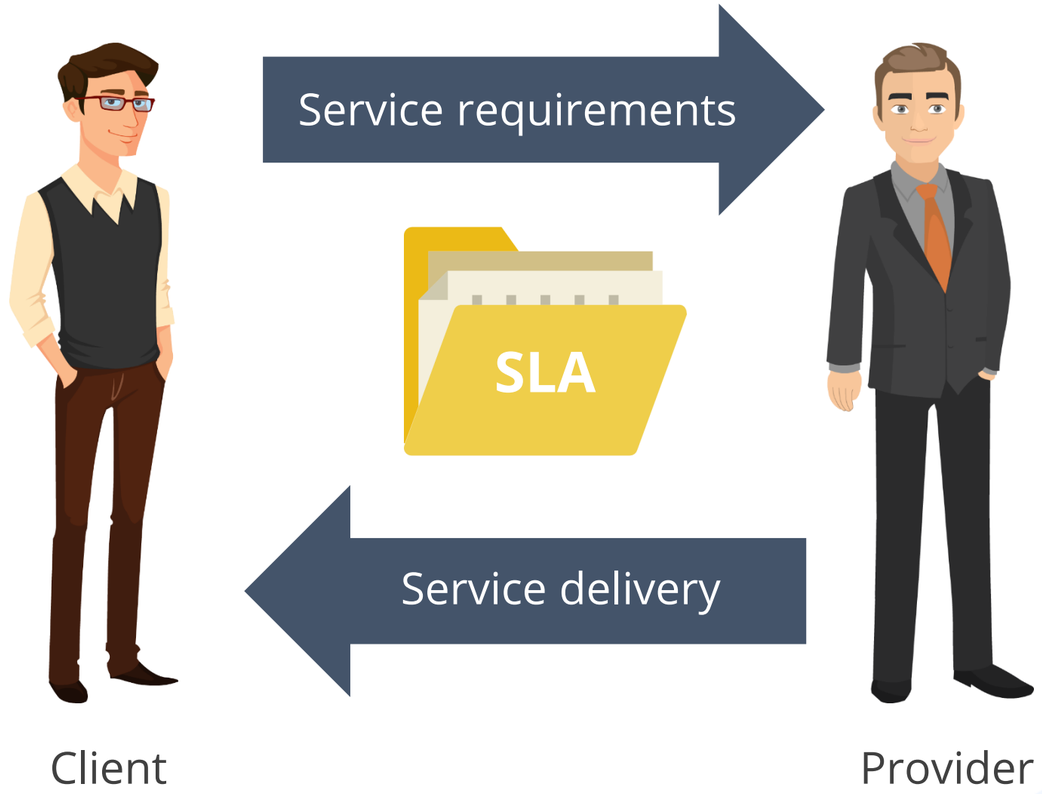
Supplier capability	Ensure supplier has good security development and management practices
Product security	Perform an assessment of the risk of the product for critical security compromise and mitigation requirements
Product logistics	Control access to the product in transit at each step in the supply chain
Operational product control	Implement appropriate configuration and monitoring controls during the operational use of the product or service

Service-Level Agreement (SLA)

It is a formally defined level of service provided by an organization.

SLAs may be defined for:

- Security incident response
- Security alert delivery
- Security investigation
- Policy and procedure review



Silicon Root of Trust (SiRoT)

It is a security concept that embeds cryptographic hardware directly into silicon chips, providing a secure foundation for various security-critical applications. Key components of SiRoT include:

Hardware-based key generation

Secure storage

Trusted execution environments (TEEs)

Software Bill of Materials (SBOM)

It is a comprehensive list of the components required to create a software product, resembling a detailed recipe. Key components of SBOM include:

- Direct dependencies
- Indirect dependencies
- Version information
- License information

Third-Party Management

A third party is a company that is not under direct business control of the organization that engages it.

A third-party relationship is any business arrangement, by contract or otherwise, between a company and another entity.

Outsourcing is the subcontracting of a business process to a third-party company.

Organizations are outsourcing systems, processes, and data to focus on core competencies, reduce costs, and speed up application deployment.

Third-party risk management is a comprehensive plan to identify and mitigate potential business and legal risks from hiring third-party services.

Third-Party Risks

These are the potential risks that an organization faces due to its reliance on external vendors, suppliers, or partners:

Information security or data privacy

A third party has insufficient experience and controls to protect the company's and customer's information from unauthorized access, disclosure, modification, or destruction.

Business continuity

A third party cannot continuously maintain its services due to business disruption (such as ineffective redundancy procedures).

Financial viability

A third party is not financially secure to continue to provide the services at acceptable levels.

Third-Party Risks

Contract compliance

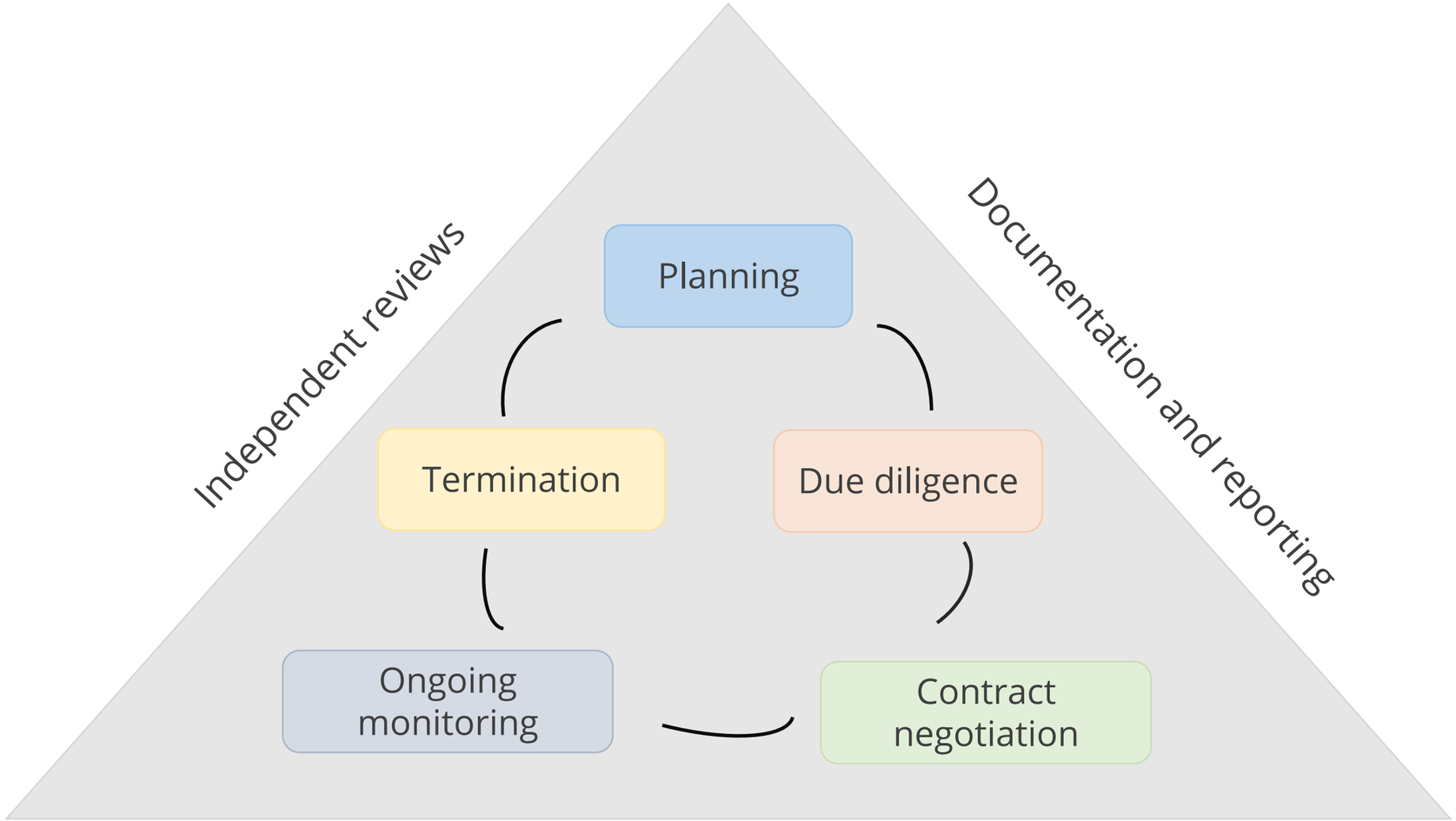
Third-party products, services, or systems are not consistent with the policies and procedures, applicable laws, regulations, and ethical standards.

Legal or regulatory

A third party lacks the necessary licenses and the expertise to keep the company compliant with domestic and international laws and regulations.

Third-Party Risk Management

The given diagram helps understand the third-party risk management.

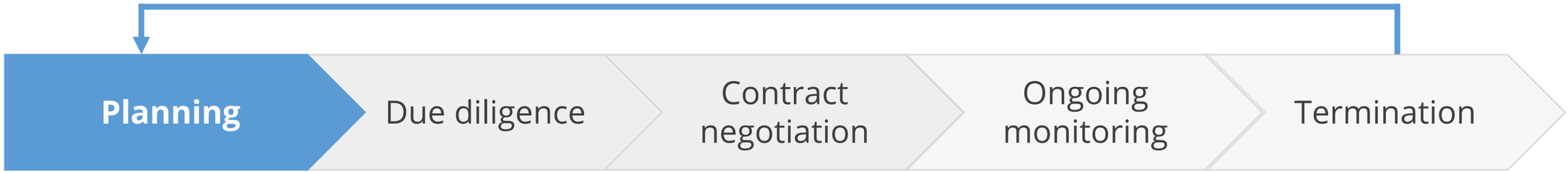


Third-Party Risk Management

The risk management plan should oversee the full life cycle of a third-party relationship including:

- The company's strategy for why it is using the third party and the inherent risks the relationship presents
- Proper due diligence in selecting the third party
- Written contracts outlining the rights and responsibilities of all parties
- Ongoing monitoring of the third party’s activities and performance
- Contingency plans for effectively terminating the relationship
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process
- Documentation and reporting to facilitate oversight, accountability, monitoring, and risk management
- Independent reviews to ensure that the processes align with the organization’s strategy and effectively manage risks

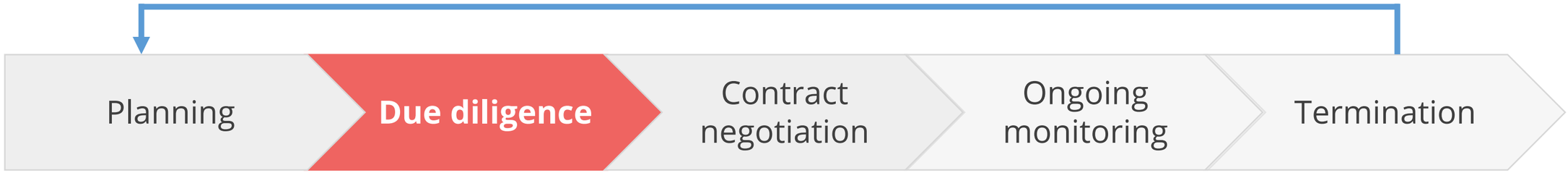
Third-Party Risk Management Life Cycle



Develop a plan to manage the relationship. This is often the first step in the third-party risk management process.

- Identify regulatory requirements
- Identify need for third-party service
- Determine inherent risks of activities
- Determine business requirements
- Analyze risk or benefit
- Incorporate risk strategy
- Establish a third-party risk profile
- Identify and qualify third parties

Third-Party Risk Management Life Cycle



Review a potential third party before signing a contract to ensure they align with the organization's risk appetite. On-site visits may be useful to fully understand their operations and capability to serve.

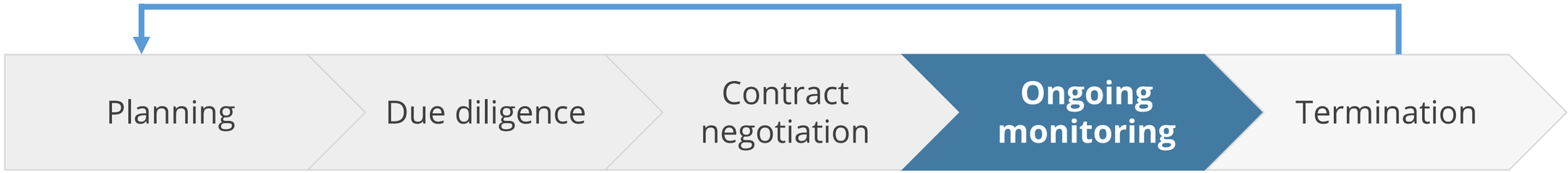
- Audited financial statements
- Business reputation and litigation
- Risk management procedures
- Compliance capabilities
- Internal audit coverage
- Information security
- Reliance on subcontractors
- Insurance coverage

Third-Party Risk Management Life Cycle

A written contract that defines the third party's expectations and responsibilities must be developed to ensure the contract's enforceability, limit the organization's liability, and mitigate performance disputes.

- Scope of the arrangement
- Performance measures or benchmarks
- Responsibilities
- Regulatory compliance requirements
- Default and termination
- Subcontracting
- Confidentiality and security
- Indemnification

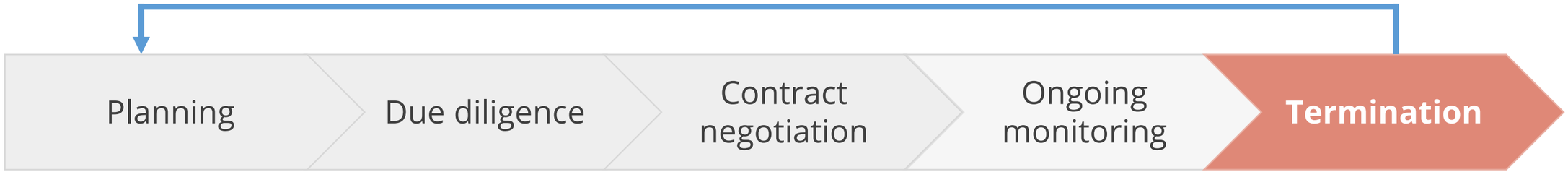
Third-Party Risk Management Lifecycle



After contracting with a third party, management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor their activities and performance.

- Process or policy review
- Ongoing performance and risk monitoring
- Ongoing due diligence and assessments
- Ongoing site visits and reviews
- Oversight and supervision
- Third-party contingency plans
- Financial reviews for viability
- Ability to recover from service disruptions

Third-Party Risk Management Lifecycle



A contingency plan must be developed to ensure a smooth transition of activities to another third party, bring the activities in-house, or discontinue the activities upon contract expiry, fulfillment, or changes to business strategy.

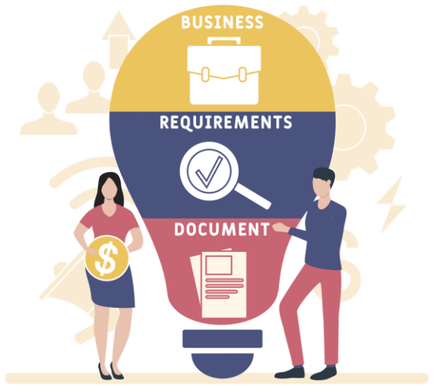
- Finalize exit strategy
- Provide notifications
- Risk exposure assessment
- Continuity planning
- Transition planning and execution
- Transfer of assets and information
- Legal confirmation of transition
- Payments, penalties, and final billings

Minimum Security Requirements

Third-party security requirements standard document sets out the minimum information security requirements expected of third parties.

- Product or service specifications must include the requirements for security controls.
- Contracts with the third party must address the identified security requirements.
- If a product’s security functionality does not satisfy specific requirements, the risk introduced must be evaluated, and additional controls must be reconsidered before purchase.
- If additional functionality causes a security risk, it must be disabled or reviewed to determine if an advantage can be taken of the available enhanced functionality.

Service-Level Requirements (SLR)



It provides the requirements for a service from a client viewpoint, defining service-level targets, responsibilities, and other specific requirements to manage the service.

A service provider prepares a service-level agreement (SLA) based on the SRL.

Quick Check

An organization is reviewing its supply chain to ensure compliance with its information security standards. Which of the following is the most effective way to achieve this compliance?

A. Periodic audits

B. Service level monitoring

C. Penetration testing

D. Security awareness trainings

Establishing Security Awareness, Education, and Training Program

Social Engineering

It is the exploitation of human behavior and trust.

It is a strategy that relies on human emotion, deceptive tricks, and outright lies.

Social engineers predate on people's intrinsic wants and needs.

They are more knowledgeable of attributes and tailor their attacks accordingly.

Social Engineering: Examples

An attacker creates an executable file that prompts a user for their password and records whatever they type.

An intruder impersonates a remote sales agent seeking help to set up remote access and contacts the help desk.

An intruder sets off a fire alarm and connects a surveillance system to a network port, while everyone is distracted.

Social Engineering: Principles

Social engineering attacks rely on one or more of the following principles to be persuasive:

Familiarity or liking

- It creates trust.
- It makes the request appear reasonable and natural.

Consensus or social proof

- It utilizes courteous behaviors.
- It creates fabricated testimonials or contacts.

Authority and intimidation

- It makes the target fearful of refusing.
- It takes advantage of a lack of knowledge or awareness.

Scarcity and urgency

- It convinces the target to make a choice.

Phishing

It is a cybercrime where attackers obtain sensitive information by pretending to be trustworthy entities.

It is a form of social engineering that often involves misleading emails, messages, or websites.

It involves distributing phishing messages to many targets in a campaign.

It varies in complexity and scale, from simple email blasts to highly targeted attacks.

It aims to compromise as many accounts or systems as possible.

Types of Phishing

Spear phishing is a scam where the attacker uses data to make an individual target more likely to be tricked.

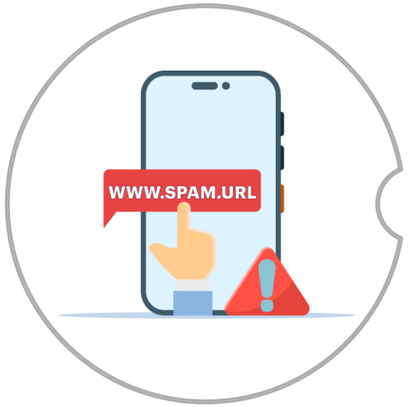
Whaling is a spear phishing attack targeting upper management in an organization.

Vishing is a phishing attack conducted through a voice channel.

Smishing uses text messages (SMS) as the attack vector.

Indicators of Phishing

Several indicators of phishing to look out for include:



Mismatched URLs

Poor grammar and spelling

Requests for sensitive information

Unsolicited attachments

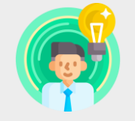
Too good to be true

Process to Counter Phishing

Isolate the threat

Analyze the content

Notify IT security

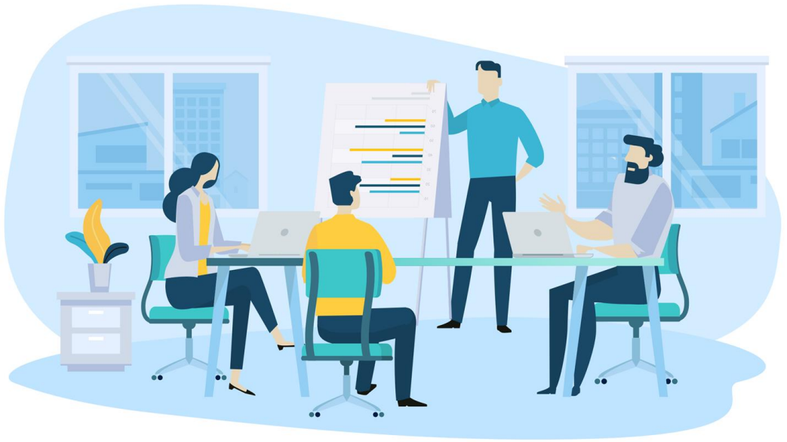


Make users aware

Update security measures

Importance of Security Awareness Training

Security awareness training is important to:



- Understand the importance of security
- Understand expected responsibilities, acceptable behaviors, and noncompliance consequences
- Modify employees’ behavior and attitude toward security
- Improve the overall security of the organization
- Implement the controls in a better way

Security Awareness Training

The given table describes the three parts of security awareness training:

Basis of distinction	Awareness	Training	Education
Objective	To focus on security	To produce required and relevant security skills and competencies	To integrate security skills and competencies into a common body of knowledge
Advantages	Organizations can inform employees about their roles and expectations in observing the information security requirements.	• Training provides guidance in the performance of particular security or risk management functions. • Training provides information on the security and risk management functions.	Educated employees can aid the organization in fulfilling security program objectives.

Implementation of Security Awareness Training Program

The following table represents the steps to develop and implement a good security awareness training program:

Basis of difference	Awareness	Training	Education
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Objective	Exposure	Skills	Understanding
Teaching	Media	Practical instructions	Theoretical instructions
Method	• Videos • Newsletter • Posters	• Lecture • Case study • Workshop • Hands-on practice	• Discussion • Seminar • Background reading • Research
Test measure	• True or false • Multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe	Short term	Intermediate	Long term

Methods and Techniques to Present Awareness and Training

Security awareness training could help organizations protect against social engineering attacks.

Organizations should identify and train a security champion within a team who then becomes an enabler and promoter of security best practices.

The security champion should be the single point of contact within a department and should act as a liaison between the security team and the employees.

Security leaders can use gamification to enhance cybersecurity training for their employees.

Employees can use a simulated environment to test and improve their readiness for cyber incidents.

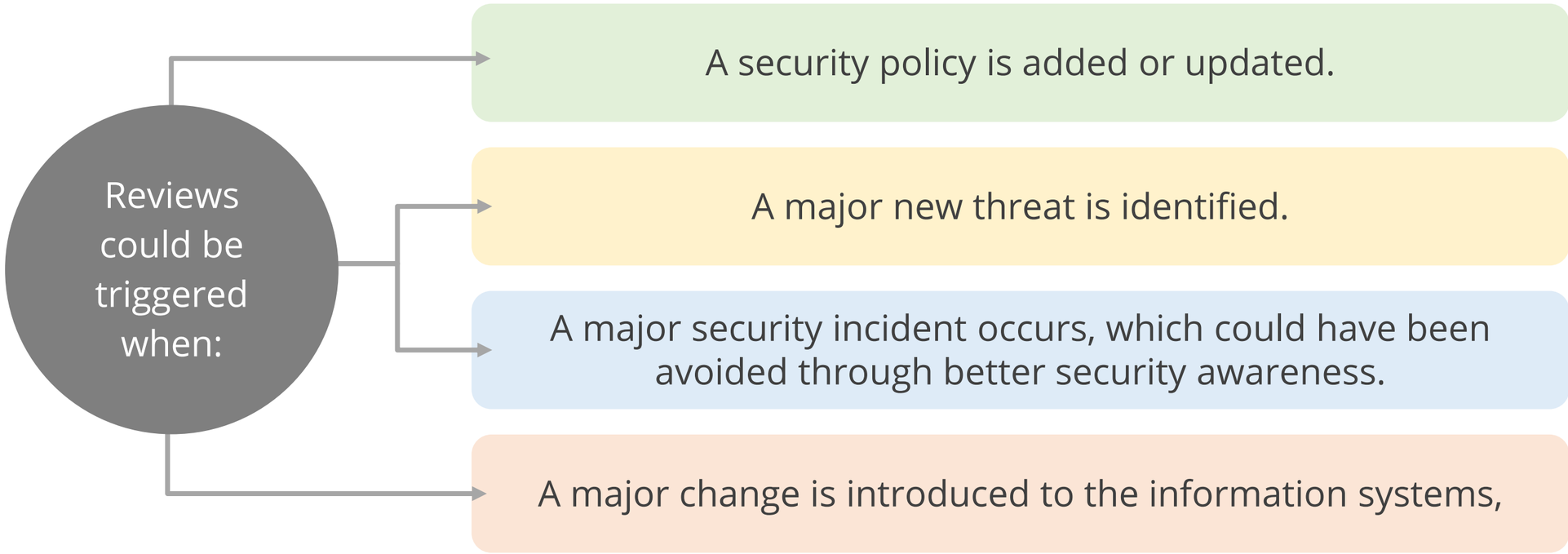
Business Scenario

PwC launches Game of Threats

- In 2016, global accountancy firm PwC launched Game of Threats to help senior executives and directors assess and enhance their readiness for cyber incidents.
- Game of Threats is an interactive digital game that simulates a real-world cyber breach to help executives better understand the steps they can take to protect their companies.
- The game was based on others' real-life experience with cyberattacks.
- Designed to be nontechnical, the game environment creates a realistic experience where participants are required to make quick, high-impact decisions with minimal limited resources.
- The participants are provided with a detailed summary of each game with a review of their strategy, actions, and missed opportunities.

Periodic Content Reviews

The training content must be periodically reviewed, kept up to date, and tailored to meet the needs of the target audience.



Program Effectiveness Evaluation

A security awareness training program is crucial for fostering a security culture within an organization and must be assessed for its effectiveness.

Calculate the return on investment (ROI) by comparing training costs to potential benefits, such as reduced losses due to security incidents

Assess knowledge retention, behavioral changes, positive attitude, reduced incidents, and cost-effectiveness

Regularly review and update the program based on evaluation results and evolving security threats

Incorporate gamification elements for more engaging training and encourage active participation during training sessions

Methods to Assess Program Effectiveness

- **Reaction**
- Learning
- Behavior
- Results

To what degree participants react favorably to the training

Sample questions:

- Was the course relevant and useful?
- Was the training enjoyable?
- Does the training accommodate their learning styles and paces?
- How likely would they recommend the course to their colleagues?

Methods to Assess Program Effectiveness

- Reaction
- Learning
- Behavior
- Results

To what degree participants acquire the intended knowledge, skills, attitudes, confidence, and commitment based on their participation in a training event

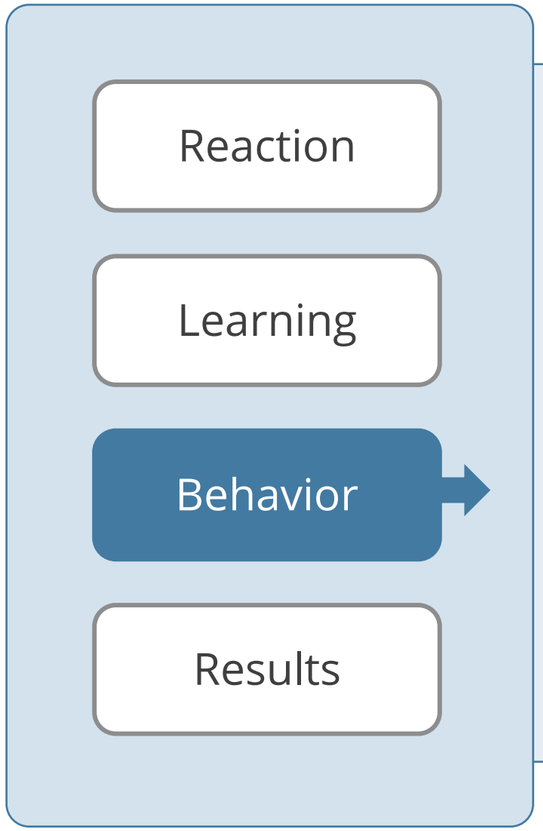
Methods:

- Use assessments or tests before and after the training to check performance changes due to the program

Sample questions:

- Has their knowledge increased as a result of the training?

Methods to Assess Program Effectiveness

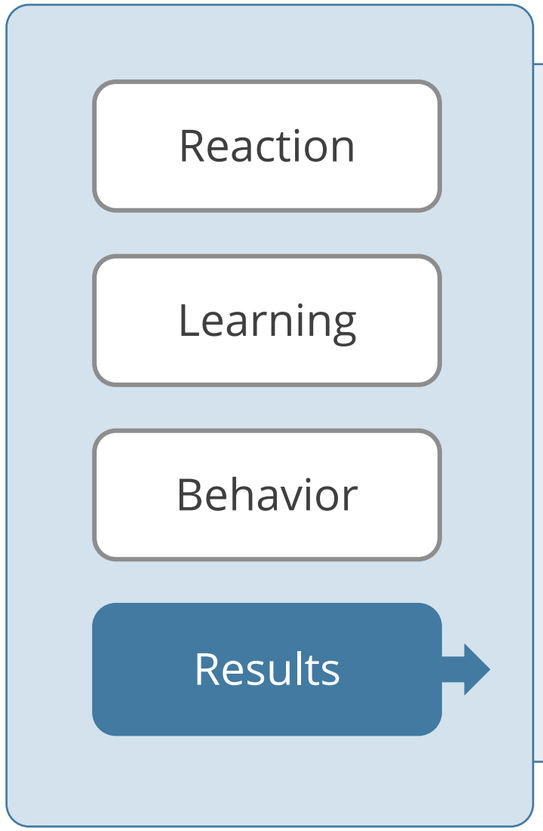


To what degree participants apply what they learned during training when they are back on the job

Sample questions:

- Have the trainees put any of their learnings to use?
- Are trainees able to teach their new knowledge, skills, or attitudes to other people?
- Are trainees aware that they have changed their behavior?

Methods to Assess Program Effectiveness



To what degree targeted outcomes occur as a result of the training event and subsequent reinforcement

Sample key metrics to measure results:

- Improved work quality and productivity
- Improved business results (such as sales, customer satisfaction, and retention)
- Increased employee engagement, satisfaction, and retention
- Reduced production cost, duration, and error and rework

AI in Cyber Security Training

AI is revolutionizing cybersecurity by efficiently processing large amounts of data, significantly impacting the training of cybersecurity professionals.

AI-powered platforms offer adaptive learning, real-time feedback, simulation training, threat intelligence, ethical training, virtual tutors, and microlearning.

AI can tailor training content to individual learners, provide immediate feedback, simulate cyberattacks, analyze threat data, and provide ethical training.

AI-powered tutors offer personalized guidance and can be easily integrated into busy schedules.

Quick Check

As a security team plans an IT security awareness program, they consider various elements for its effectiveness. What is the most important success factor in designing this program?

A. Content is tailored to the target attendees.

B. It is represented by senior management.

C. Employees across all hierarchical levels are trained.

D. It is focused on hands-on-training rather than theoretical knowledge.

Key Takeaways

- Information security governance provides strategic direction and ensures security objectives are achieved.
- Security policy guides the security program in the organization.
- Information risk management is the process of identifying and assessing the risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain it at that level.
- When selecting the right control to reduce a particular risk, the functionality, viability, and the available budget must be assessed. Also, a cost-benefit analysis must be performed.
- Computer crimes refer to any crime that involves a computer and a network.
- An organization’s ability to respond to any disaster and recover from disruptions depends on the business continuity plan (BCP).

Thank You