Certified Information Systems Security Professional (CISSP) Certification Training Course

Domain 01: Security and Risk Management

Learning Objectives

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

- Recognize the importance of information security management
- Describe security policy implementation
- Describe information risk management
- Define personnel security and security function management process
- Define computer crime
- Explain the BCP process

Introduction to Domain 1: Security and Risk Management

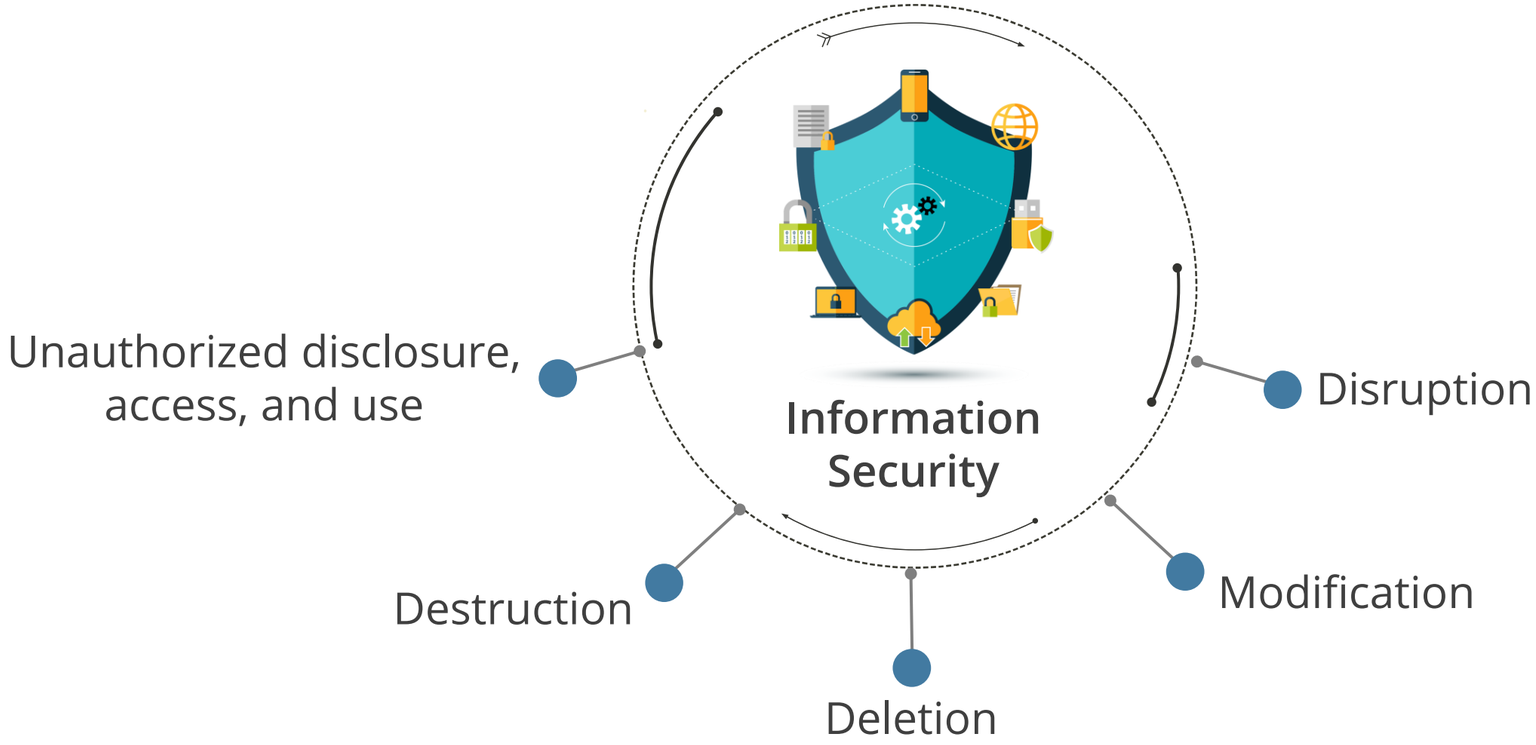
Importance of Information Security and Risk Management

Kevin Butler is a Security Administrator in the network firewalls division at Nutri Worldwide Inc. He must prepare for the CISSP exam. He starts his preparation by reading a historical case of a competitor.

The competitor company had failed to understand the importance of information security. The company had planned their Business Continuity Plan (BCP) without continuous involvement of IT.
IT security input was taken without the team playing an active role. The BCP was weak in the area of IT security. When the headquarters of the competitor company was hit by a tornado, there was a huge information leak as data protection measures were not well planned at the time of the natural disaster. The IT department tried their best to prevent this. The company faced major losses, which led them to file for bankruptcy within a few years.

Introduction to Information Security

Information security is the process of protecting information and information systems from the following:



Introduction to Information Security

Factors that impact information security:

Technology

- Platforms and tools used
- Network connectivity
- Level of IT complexity
- New or emerging security tools
- Operational support for security

Business plans and general business environment

- Nature of business
- Risk tolerance
- Industry trends
- Merger acquisitions and partnership
- Outsourcing service or providers

Cybersecurity

What is Cybersecurity?

- Cybersecurity refers to anything intended to protect enterprises from intentional attacks, breaches, incidents, and consequences
- It can also be defined as the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems

Why is Cybersecurity important?

- Due to technological advancement, the rate of cybercrime is increasing
- As most of the business happens online these days, there is an increasing demand to protect this data
- Presence of crime syndicates
- Cyber armies
- Financial fraud

Difference between Information Security and Cybersecurity

Information Security

- Information security deals with information regardless of its format.
- It encompasses paper documents, digital data, and intellectual property.

Cybersecurity

- It can be defined as the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.
- Cybersecurity is a component of information security.

Terrifying Cybercrime Statistics

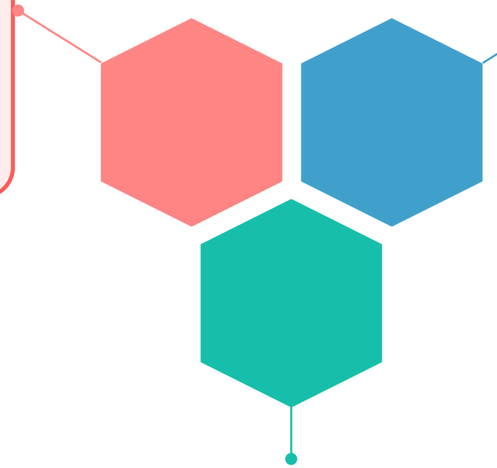
Recent trends which make Cybersecurity more important:

- During the first six months of 2018, more than 25 million records were compromised or exposed every day
- Over 24,000 malicious mobile apps are blocked daily
- Ransomware attacks on the healthcare industry will quadruple
- Cybercrime to cost $6 trillion by 2021
- 300 billion passwords worldwide by 2020
- More than 60% of fraud originates from mobile devices
- Personal data sells for as little as $0.20
- 90% of hackers use encryption

Approaches to Cybersecurity

Compliance based

Relies on regulations or standards to determine security implementation



Ad hoc

This approach simply implements security with no rationale or criteria

Risk based

This approach relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk

Understand, Adhere to, and Promote Professional Ethics

(ISC)^2 Code of Professional Ethics

The (ISC)^2 Code of Professional Ethics has two categories:

Code of Ethics Preamble

- The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, 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.

Organizational Code of Ethics

Ethics are the principles and values used by an individual to govern his or her actions and decisions.

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

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.

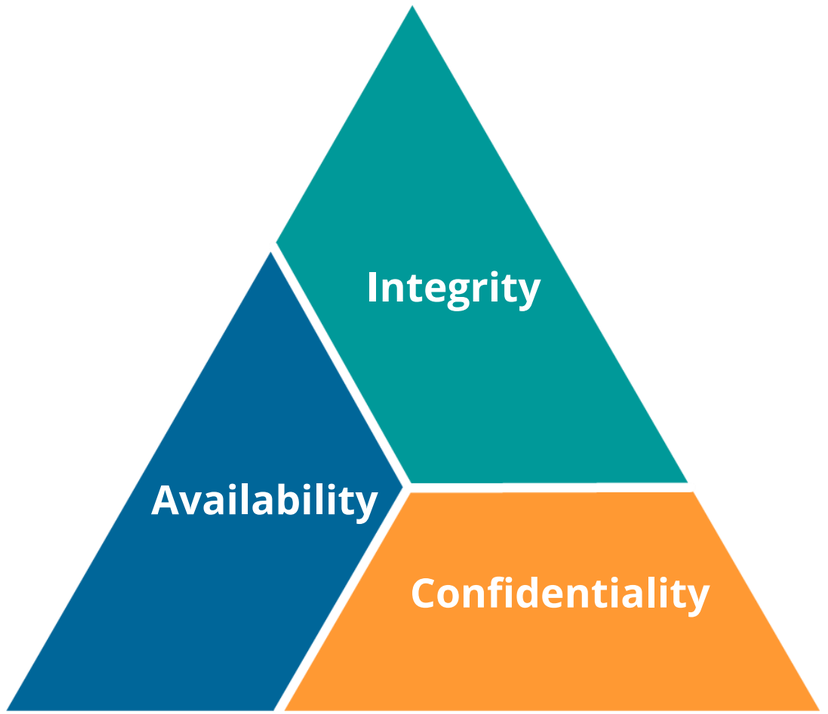
A code of ethics can help your organization to:

- Show customers that it values integrity
- Define the terms of ethical standard of behavior at work
- Guide decision-making in difficult situations

Understand and Apply Security Concepts

Role and Importance of CIA in Information Security

Confidentiality, Integrity, and Availability (CIA) have served as the industry standard for computer security since the time of the first mainframes.



CIA Triad: The three principles of security

Confidentiality

The principle of confidentiality asserts that information and functions can be accessed only by authorized parties.

Example: Military secrets

Threats to Confidentiality:

- Hackers
- Masqueraders
- Unauthorized user activity
- Unprotected files downloaded
- Unprotected networks
- Unauthorized programs
- Social engineering attacks

Integrity

The principle of integrity asserts that information and functions can be added, altered, or removed only by authorized people and means.

Example: Incorrect data entered by the user into a database

Threats to Integrity:

- Hackers
- Masqueraders
- Unauthorized user activity
- Unprotected files downloaded
- Unprotected networks
- Unauthorized programs
- Social engineering attacks
- Authorized subjects corrupting data and programs accidentally or intentionally

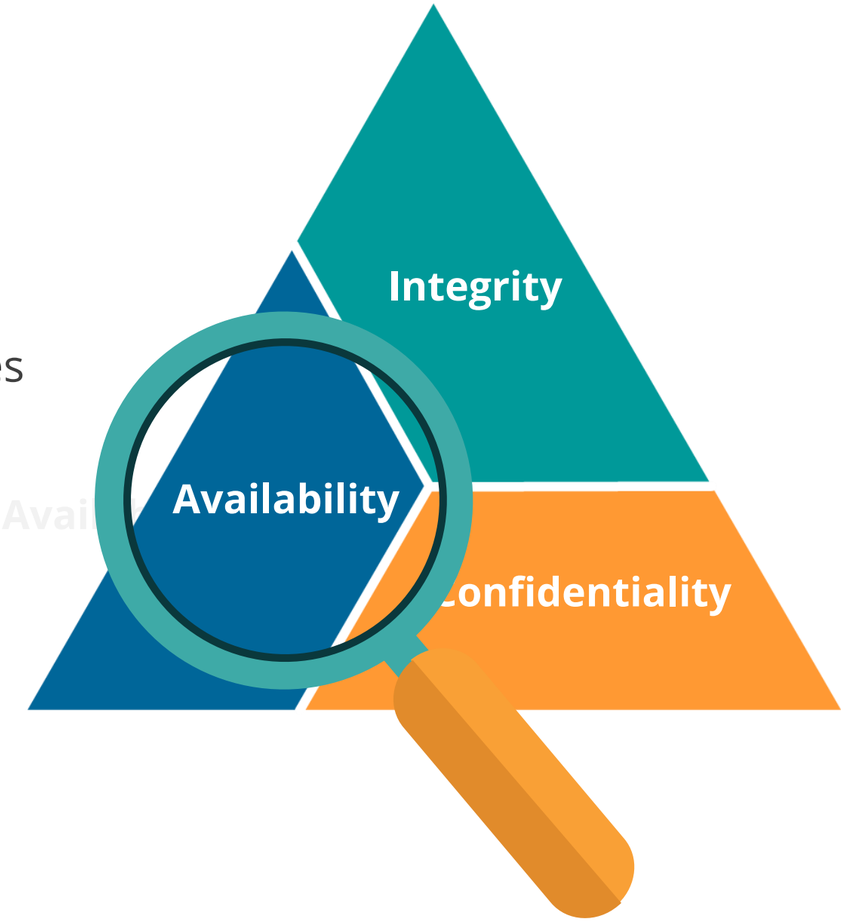
Availability

The principle of availability asserts that systems, functions, and data must be available on-demand according to the agreed-upon parameters based on levels of service.

Example: Network Load Balancing

Threats to Availability:

- Denial of service
- Distributed denial of service attacks
- Natural disasters like fire, floods, storms, or earthquakes
- Human actions like bombs or strikes



Evaluate and Apply Security Governance Principles

Information Security Management

Information Security Management

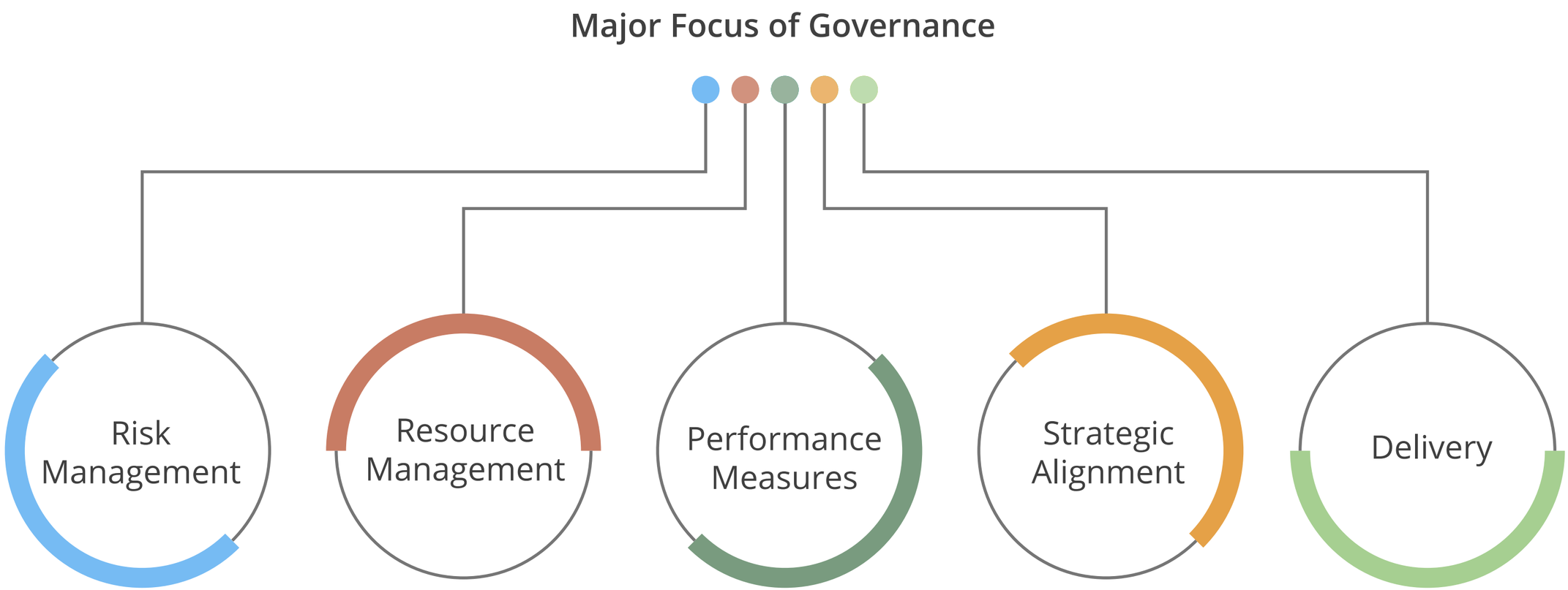
- Information Security Management describes the controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.
- It also includes information risk management which is a process that involves the assessment of the risks an organization must deal with in order to manage and protect the assets, as well as the dissemination of other risks to all appropriate stakeholders.

Information Security Management

Information security management ensures the implementation of the following:

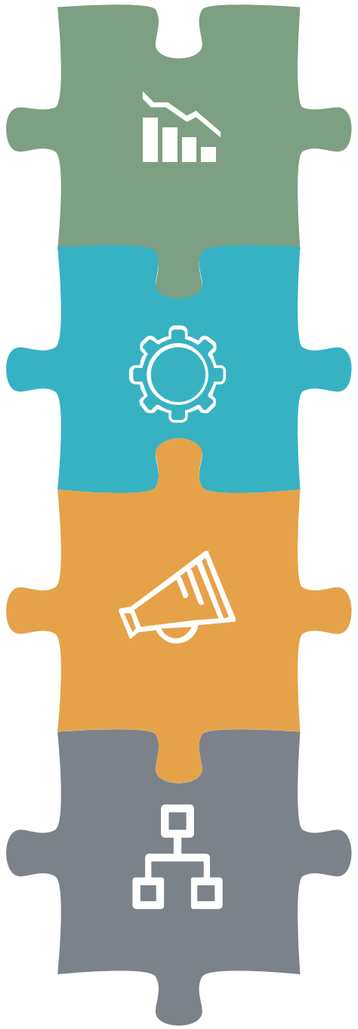
- Information security policies
- Standards
- Procedures
- Guidelines
- Baselines
- Information classification
- Risk management
- Security organization
- Security education

Information Security Governance



Information Security Governance

Information Security Governance is intended to guarantee



- Risks are reduced
- Appropriate information verifying that security activities are being performed
- Information security investments are appropriately directed
- The executive management can determine program effectiveness

Governance, Risk Management, and Compliance (GRC)

Introduction to GRC

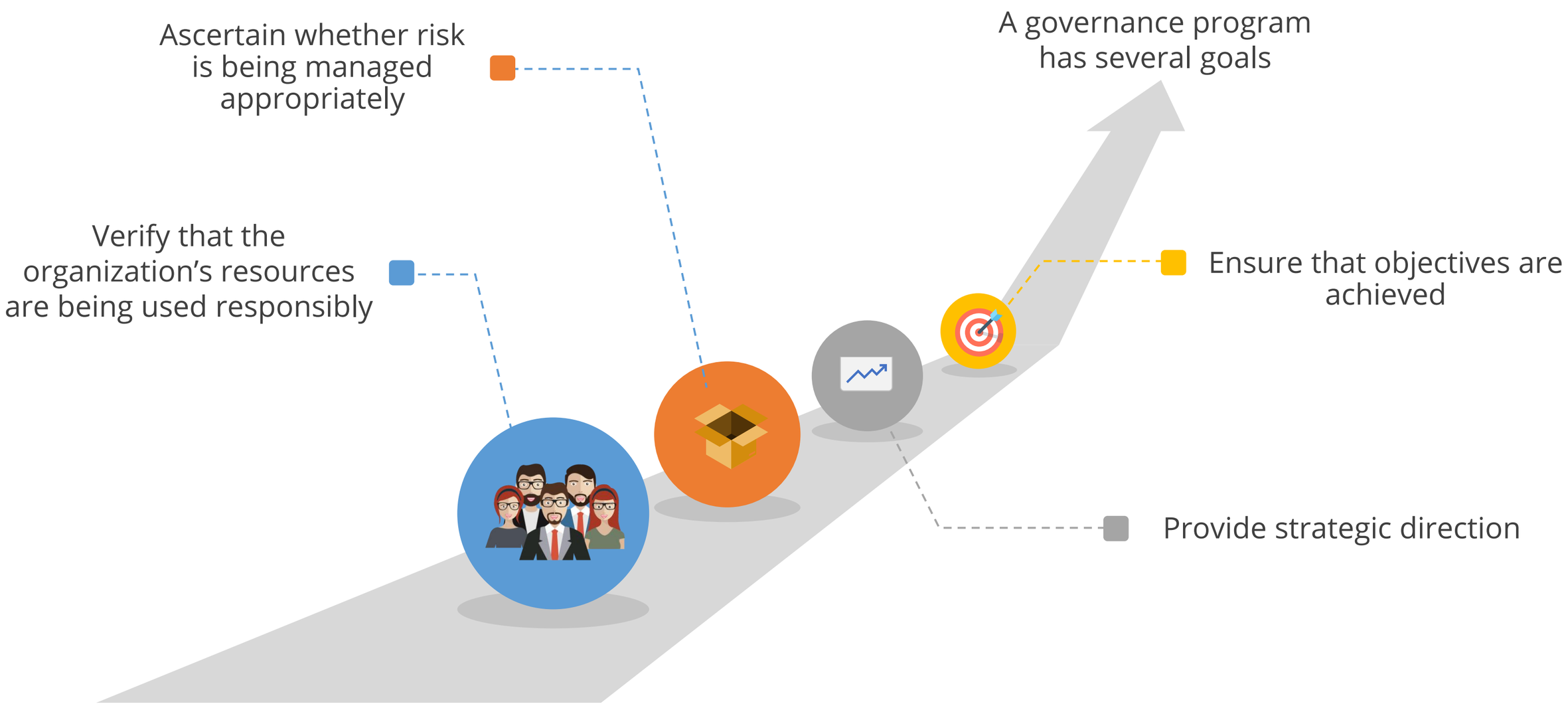
- GRC stands for Governance, Risk Management, and Compliance.
- The GRC of every organization is different and varies based on the type of organization.
- It depends on an organization's mission (business), size, industry, culture, and legal regulations.
- Ultimate responsibility of GRC program is to protect their assets and operations, including their IT infrastructure and information.

Governance, Risk Management, and Compliance (GRC)

Governance

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

Governance, Risk Management, and Compliance (GRC)



Governance, Risk Management, and Compliance (GRC)

Risk Management

- Risk Management 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, and cyber risk.

Compliance

- Compliance is the act of adhering to, and 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.

Business Scenario

Kevin is studying the importance of Information Security Governance and Management.

- Governance is associated with providing an oversight, enacting policies, establishing accountability, and planning resources and strategies.
- Management on the other hand involves implementing strategies, enforcing policies, handling responsibilities, and planning resources and the project.

Doing the right thing is *Management*; doing things right is *Governance*.

Question: Is this statement true?

Business Scenario

Kevin is studying the importance of Information Security Governance and Management.

- Governance is associated with providing an oversight, enacting policies, establishing accountability, and planning resources and strategies.
- Management on the other hand involves implementing strategies, enforcing policies, handling responsibilities, and planning resources and the project.

Doing the right thing is *Management*; doing things right is *Governance*.

Question: Is this statement true?
Answer: It is not true. The correct statement would be: Doing the right thing is Governance. Doing things right is Management.

IT Security and Organizational Goals, Mission, and Objectives

Goal, mission, and objective:

1

Define what the organization desires to achieve

2

Help in creating long term and short-term strategies

3

Indicate how it will proceed to achieve them

Goals, Mission, and Objectives

The definition of goals, mission, and objectives is as follows:

Objectives

The map used to reach the goals of the organization

Mission

Provides the overall context for what the organization wants to accomplish

Goals

A statement of the organization's purpose and reason for existence

Aligning Security with Goals, Mission, and Objectives

Information security can be aligned with organizational goals, mission, and objectives in two ways.

Reducing Risk

- Protect the organization's assets and processes through appropriate activities and controls.
- Be 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.

Business Scenario

Kevin has understood the importance of the mission, goals, and objectives of his organization and the importance of aligning its security to these.

He read the following statement on the company website.

"Nutri Worldwide Inc. will pursue and foster opportunities for growth and enrichment for its employees and stakeholders with the customer being the focal point."

Question: Is this a mission, goal, or objective statement?

Business Scenario

Kevin has understood the importance of the mission, goals, and objectives of his organization and the importance of aligning its security to these.

He read the following statement on the company website.

> "Nutri Worldwide Inc. will pursue and foster opportunities for growth and enrichment for its employees and stakeholders with the customer being the focal point."

Question: Is this a mission, goal, or objective statement?

Answer: It is a mission statement.

Control Framework

- Control framework is a data structure that comprises a set of an organization's internal controls, that is, 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.
- The control framework 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.
- Example:
  - COBIT (Control Objectives for Information and Related Technologies)
  - ISO 17799/27001

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
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

Control Objectives for Information and Related Technologies (COBIT)

COBIT

- Issued by ISACA® (Information Systems Audit and Control Association), which is a nonprofit organization for IT governance
- Main function of COBIT is to help a company 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

ISO 27001:2013

ISO/IEC 27001

- An internationally recognized and structured methodology dedicated to information security
- A management process to evaluate, implement, and maintain an information security management system (ISMS)
- A comprehensive set of controls comprised of the best practices in information security

ISO 27001 Domains

- Security policies
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance

ISO 27001:2013

ISO/IEC 27001

- Can be applicable to all industry sectors
- Emphasizes prevention
- ISO 27001 has 114 controls mapped to 14 security domains

ISO 27001 Domains

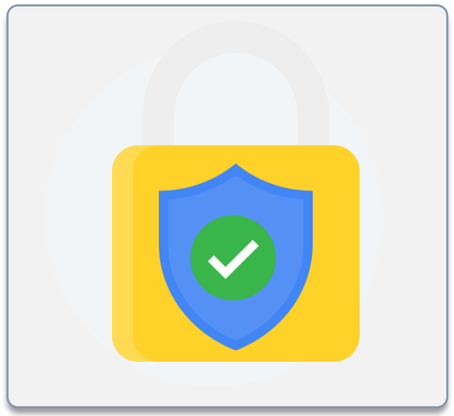
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Due Care

It’s a legal term. It 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



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

Taken 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

Due diligence might not be legally liable. It:

- Is the act of understanding and investigating the risks the company faces
- Means practicing the activities that maintain the due care efforts
- 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, security controls should be regularly monitored and rules should be updated depending on the requirement

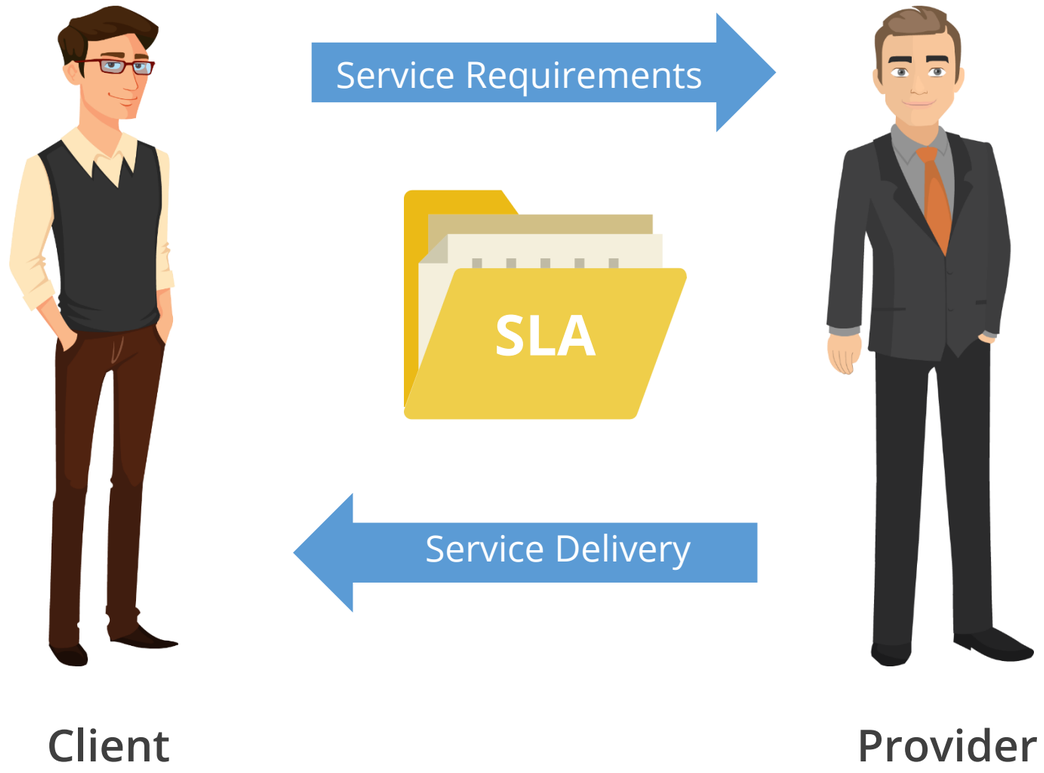
Determine Compliance and Other Requirements

Service-Level Agreement

Service-level agreement (SLA) 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



Managing Third-Party 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

Offshoring: Privacy Requirements and Compliance

- Offshoring is outsourcing to another country.
- Offshoring can increase privacy and regulatory issues.

Example: Data offshored to India by a U.S 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 U.S. Medical Transcription organization's data is offshored can agree to follow HIPAA rules via a contract.

Understand Legal and Regulatory Issues that Pertain to Information Security in a Holistic Context

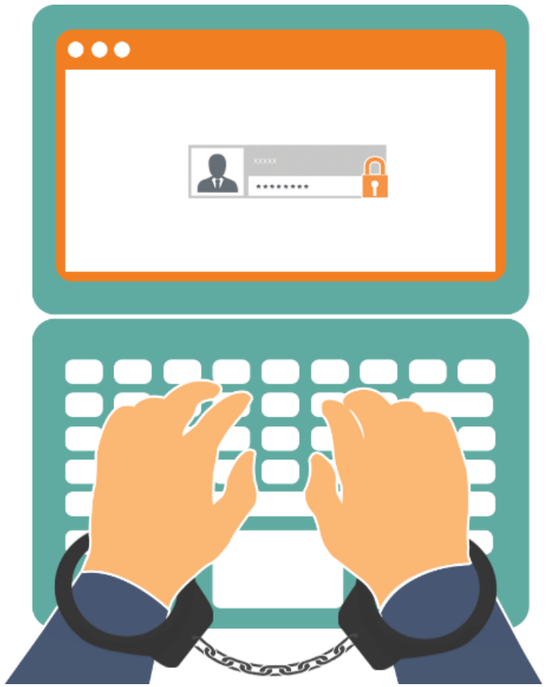
Computer Crimes

Cybercrime: Definition

Cybercrimes are defined as *offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks, such as the Internet, through chat rooms, emails, notice boards, groups, and mobile phones through SMS or MMS.*

Introduction to Computer Crimes

- Any crime that 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



Introduction to Intellectual Property (IP) Law

- Intellectual property laws are designed to protect both the tangible and intangible items and properties.
- The main goal is to protect properties from those who want to copy or use it without due compensation to the inventor or creator.

Types of Intellectual Property (IP) Law

Patent

- A patent grants the owner a legally enforceable right to exclude others from practicing the invention.
- A patent is applicable for 20 years.
- A patent protects new, useful, and nonobvious inventions.
- After the expiry of a patent, the invention is open to the public domain.
- Three requirements that need to be satisfied are:
  - The invention should be new and an original idea
  - The invention must be useful
  - The invention must not be obvious

Trademark

- Trademark laws protect the goodwill a merchant or vendor invests in the products.
- A trademark grants exclusive rights to the owner of the trademark.
- A trademark consists of any word, name, symbol, color, sound, product shape, device, or a combination of these.
- Trademarks are registered with a government registrar.
- One trademark must not be similar to another trademark.
- The trademark should not be descriptive of the goods or service that you will offer.

Types of Intellectual Property (IP) Law

Copyright

- A copyright covers the expression of ideas
- It 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 provided protection for 95 years from the first publishing date or 120 years from the date of creation, whichever is shorter.

Trade Secret

- Trade secret law protects certain types of information or resources from unauthorized use or disclosure.
- A trade secret is something that is proprietary to a company and important for its survival and profitability.
- Examples include 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.
- You can protect a trade secret by having your own control structures depending on the type of trade secret and by making your employees sign an NDA.

Digital Millennium Copyright Act (DMCA)

Digital Millennium Copyright Act (DMCA)

- The Digital Millennium Copyright Act (DMCA) is a controversial United States digital rights management (DRM) law. The intent behind DMCA was to create an updated version of the copyright laws to deal with the special challenges of regulating digital material.
- Nonprofit organizations are exempted from this act.

DMCA Takedown Notice

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

Types of Intellectual Property (IP) Laws

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.

Business Scenario

Kevin Butler was studying about intellectual property laws as a part of his preparation for the CISSP exam. While studying the topic, he remembered a recent case in which his organization had successfully won a lawsuit against a competitor organization.

The case in question was regarding the use of Nutri Worldwide Inc.'s product name for a similar product by the competitor organization.
The court gave its verdict in favor of Nutri Worldwide Inc., and the opposite party had to pay a heavy fine.

Question: Under which type of IP law was the lawsuit filed?

Business Scenario

Kevin Butler was studying about intellectual property laws as a part of his preparation for the CISSP exam. While studying the topic, he remembered a recent case in which his organization had successfully won a lawsuit against a competitor organization.

The case in question was regarding the use of Nutri Worldwide Inc.'s product name for a similar product by the competitor organization.
The court gave its verdict in favor of Nutri Worldwide Inc., and the opposite party had to pay a heavy fine.

Question: Under which type of IP law was the lawsuit filed?

Answer: The dispute was over the violation of Nutri Worldwide Inc.'s trademark.

Import or Export Controls and Transborder Data Flow

Following are the basic concepts of import or export controls and transborder data flow:

Import or Export Controls

- They ensure that software complies with the local laws.
- A few software applications are illegal to import or export, for example an encryption software.
- The United Nations Security Council (UNSC) can impose sanctions on any country as voted on by member nations of the council. Due to the sanctions, the technology transfer to these countries is strictly prohibited.

Transborder Data Flow

- It involves transfer of data from one country to another.
- An information security professional should understand the jurisdiction over the data when it moves from one country to the other.

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.

Collection limitation → Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

Data quality → Personal data should be relevant, necessary, accurate, complete, and up-to-date.

Purpose specification → The purpose for which the data is used should, in principle, be specified at the time of the collection.

Use limitation → Personal data should in principle not be used for purposes other than those specified at the time of the collection, except in certain cases.

OECD Privacy Principles

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

Security Safeguards → Personal data should be protected by reasonable security safeguards.

Openness → Data collection and processing should be transparent to the individuals.

Individual Participation → Individuals should have the right to access personal data and have the data erased, rectified, completed, or amended.

Accountability → A data controller should be accountable for complying with the implemented measures.

General Data Protection Regulation (GDPR)

The **EU General Data Protection Regulation (EU GDPR)** is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within the EU.

Companies that collect data on citizens in the European Union (EU) countries will need to comply with strict new rules for protecting customer data from the May 25, 2018.

Noncompliant organizations may face administrative fines up to €20 million or up to 4% of the entity's global turnover of the preceding financial year, 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 existing *right to be forgotten* provisions, people who don't want certain data about them online can request companies to remove it.

GDPR: Roles and Responsibilities

- A **data subject** is an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- A **data controller** is the legal entity who either alone or jointly determines the purpose for and manner in which 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),** established in each EU member state, has been tasked to enforce the GDPR and monitor the application of GDPR rules to protect individual rights with respect to the processing and transfer of personal data within the EU.

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.

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality

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

Data Protection Principles

Lawfulness, fairness, and transparency

Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Purpose limitation

Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data minimization

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Data Protection Principles

Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitations

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Business Scenario

A regulatory authority is required by an enactment to carry out certain functions, including the handling of complaints from members of the public who have environmental concerns.

Given the large number of complaints it receives, a regulatory authority provider decides to outsource its complaints handling department to a much larger regulatory authority provider with a better logistical capacity and most of its staff will second the larger authority.

The two authorities put an agreement in place stating that all data protection compliance responsibilities have been passed over to the larger authority.

Question: Is the larger authority provider a data controller or a data processor?

Business Scenario

A regulatory authority is required by an enactment to carry out certain functions, including the handling of complaints from members of the public who have environmental concerns.

Given the large number of complaints it receives, a regulatory authority provider decides to outsource its complaints handling department to a much larger regulatory authority provider with a better logistical capacity and most of its staff will second the larger authority.

The two authorities put an agreement in place stating that all data protection compliance responsibilities have been passed over to the larger authority.

Question: Is the larger authority provider a data controller or a data processor?

Answer: The larger authority provider is a data processor acting on the instruction of the regulatory authority.

Understand 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

Investigation Types: Civil Investigation

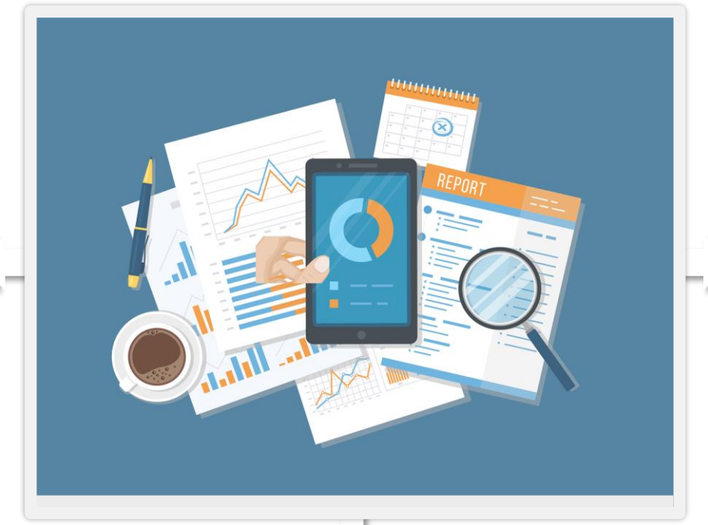
Civil investigation deals with offense committed against individuals or companies that result in damages or loss.

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

Investigation Types: Administrative Investigation

Administrative investigation is explained as:

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



Administrative investigation may be initiated in response to complaints, mishaps, misconduct, or violation of organization's policy.

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

Investigation Types: Regulatory Investigation

Regulatory investigations involve determining whether a regulatory law has been violated.

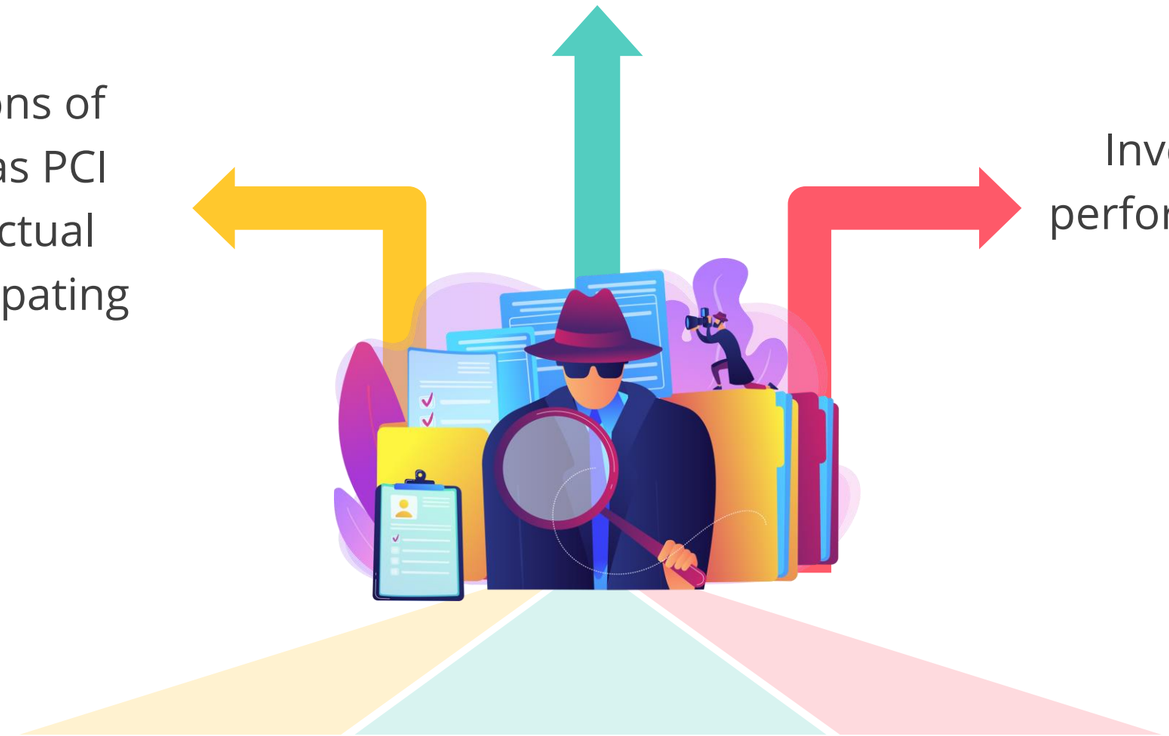
Regulation is a law established by the government body.

Initial inquiries range from an informal phone call seeking limited information to a full-blown regulatory investigation with subpoenas seeking 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.

Business Scenario

Kevin Butler was studying the major legal systems, which are followed throughout the world. He then thought of going through the archives of legal cases involving Nutri Worldwide Inc.

He came across a recent case where Nutri Worldwide Inc. lost a legal battle against one of its partner organizations. The dispute was regarding breach of some clause of the partner agreement. The partner filed a lawsuit against Nutri Worldwide Inc. for violation of its rights and claimed a compensation of $2 million.

Question: Under which type of law had the partner filed the lawsuit?

Business Scenario

Kevin Butler was studying the major legal systems, which are followed throughout the world. He then thought of going through the archives of legal cases involving Nutri Worldwide Inc.

He came across a recent case where Nutri Worldwide Inc. lost a legal battle against one of its partner organizations. The dispute was regarding breach of some clause of the partner agreement. The partner filed a lawsuit against Nutri Worldwide Inc. for violation of its rights and claimed a compensation of $2 million.

Question: Under which type of law had the partner filed the lawsuit?

Answer: The partner had filed the lawsuit under the Civil Law.

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Security Policies

Security policy 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 be generic, non-technical, and easily understood.

It must integrate security into all business processes and functions.

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

It must support the vision and mission of the organization.

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.

Standard policy components	Purpose statement, policy objectives, resources provision, staff allocation, and guidelines and standards
Policy elements	Purpose, scope, responsibilities, and compliance
Policy creation guidelines	Assigning a principal function to be responsible for control, compliance with policy as a condition of employment, and avoiding exceeding two pages and use generic terms

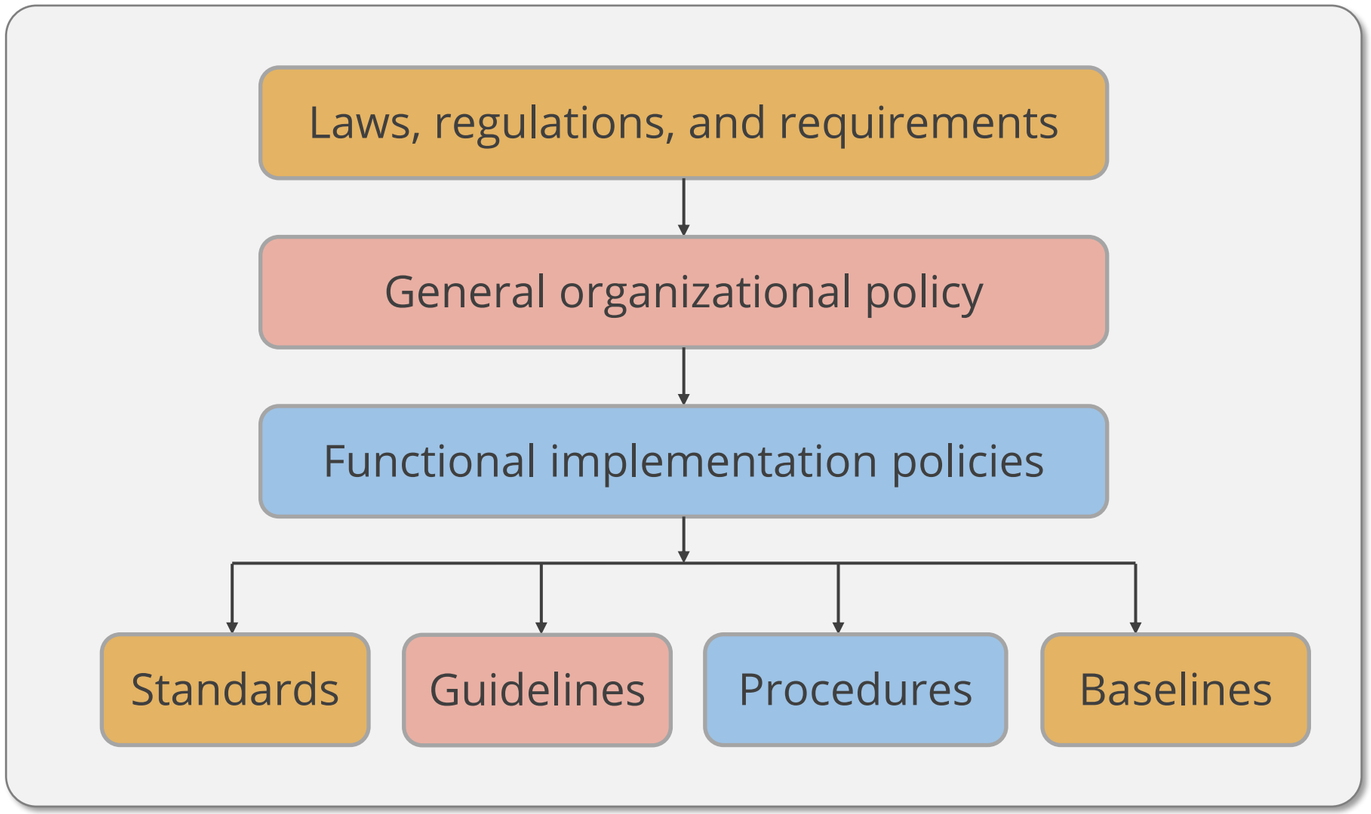
Security Policy Implementation

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

Management responsibilities for policy	Protecting resource assets within the company's control, implementing security in accordance with the company policy, and initiating corrective actions for security violations
Policy enforcement	Avoiding errors that can lead to legal challenges and ensuring compliance with policy

Policy Chart

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



Standards, Guidelines, Procedures, and Baselines

Standards

- Refers to the mandatory activities, rules, actions, or regulations
- Defines compulsory requirements
- Provides a course of action for uniform deployment of technology
- Are tactical documents
- Example: ISO 27001

Guidelines

- Refers to the recommended operational guides or actions provided to the users, operations staff, IT staff, and others
- Are flexible and can be customized for each unique system
- Serves as operating guides
- Are not mandatory statements
- Example: Security password guideline

Standards, Guidelines, Procedures, and Baselines

Procedures

- Refers to the step-by-step tasks to be performed to achieve a certain objective
- Forms the final elements of the formalized security policy structure
- Are system and software specific
- Example: Incident response procedure

Baseline

- Defines minimum level of security that every system must meet
- Are system-specific
- Establishes common secure states
- Refers to a stage or state that is used as a comparison for future changes (reference point)
- Example: All Windows 7 systems must have SP1 installed

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

Need for Business Continuity Planning

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 lives of employees

Minimize the disruptions

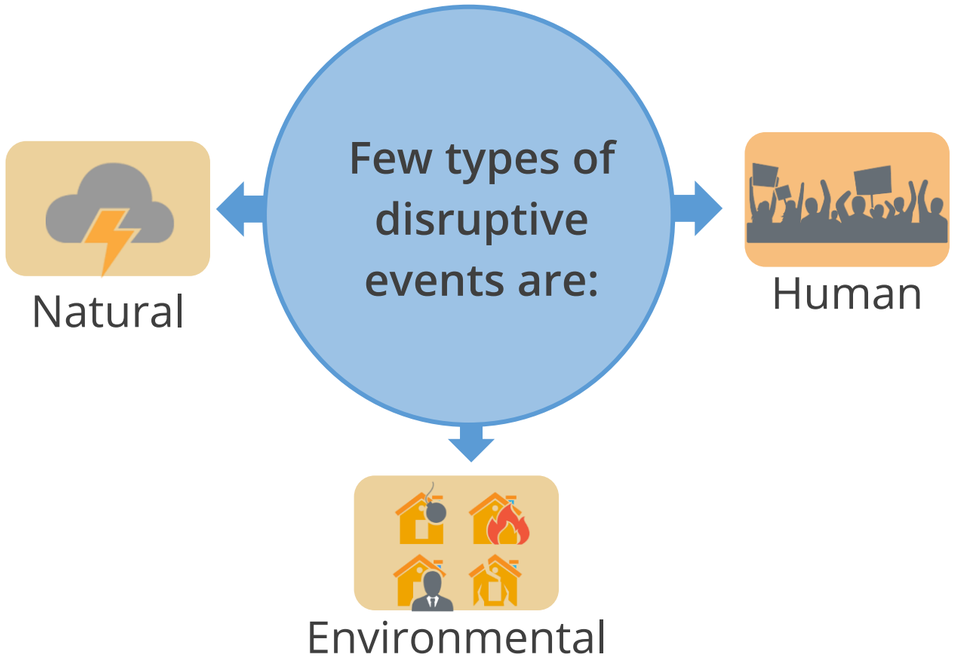
Restore normal business

Prevent financial losses

Basic Concepts: Disruptive Events

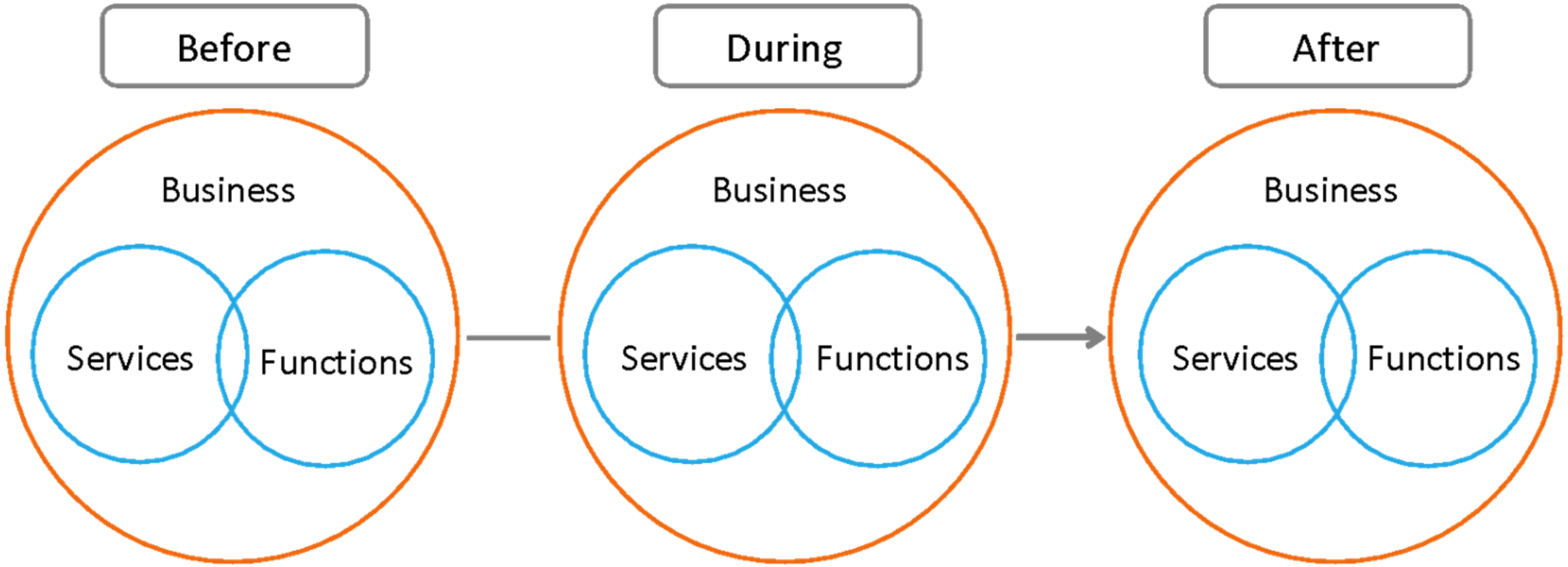
Any incident, act, or occurrence that suspends normal operations can be termed as a disruptive event or disaster.

- Disruptive events can be intentional or unintentional.
- BCP aims at minimizing the effects of a disruptive event 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

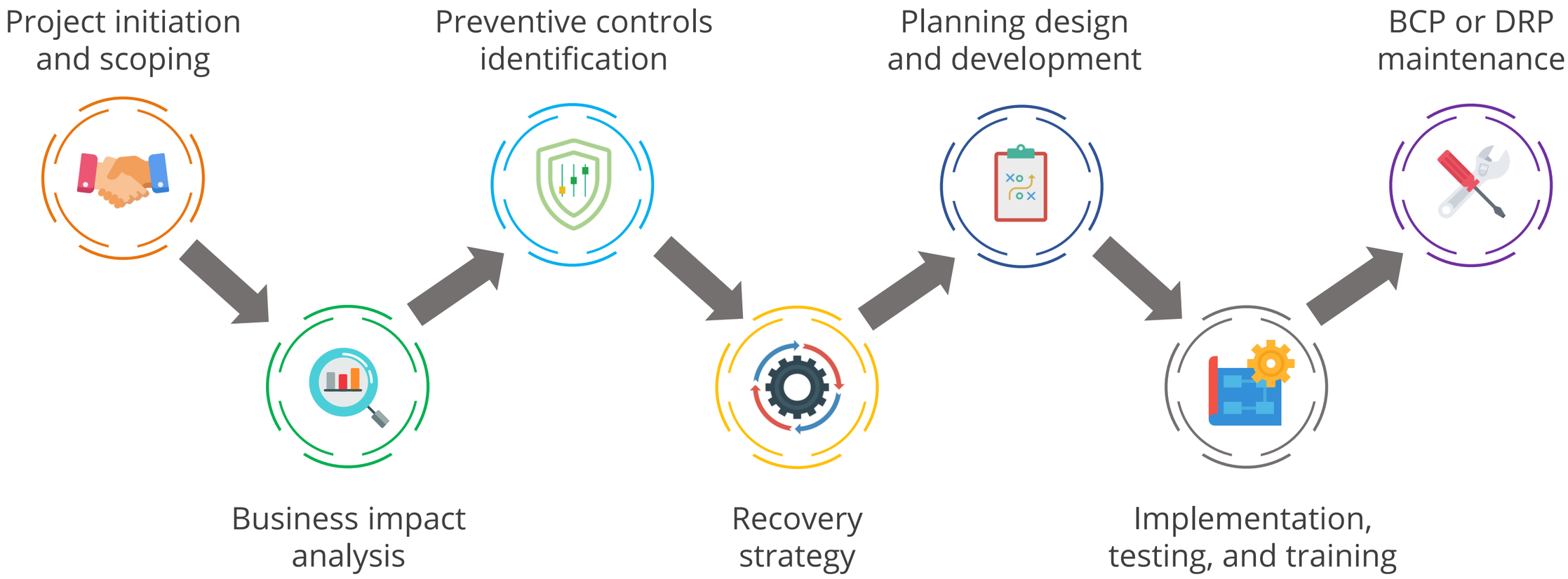
The organization's ability to respond to any disaster and recover from disruptions depends on Business Continuity Planning (BCP) or Disaster Recovery Planning (DRP) as it:

- 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

According to NIST 800-34, project initiation and scoping is the first step to achieve a comprehensive BCP or DRP.

Recent trends which make Cybersecurity more important:

- 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)

According to NIST 800-34, business impact analysis is the second phase to achieve a comprehensive BCP or DRP.

The Business Impact Analysis (BIA):

- 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
- 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**

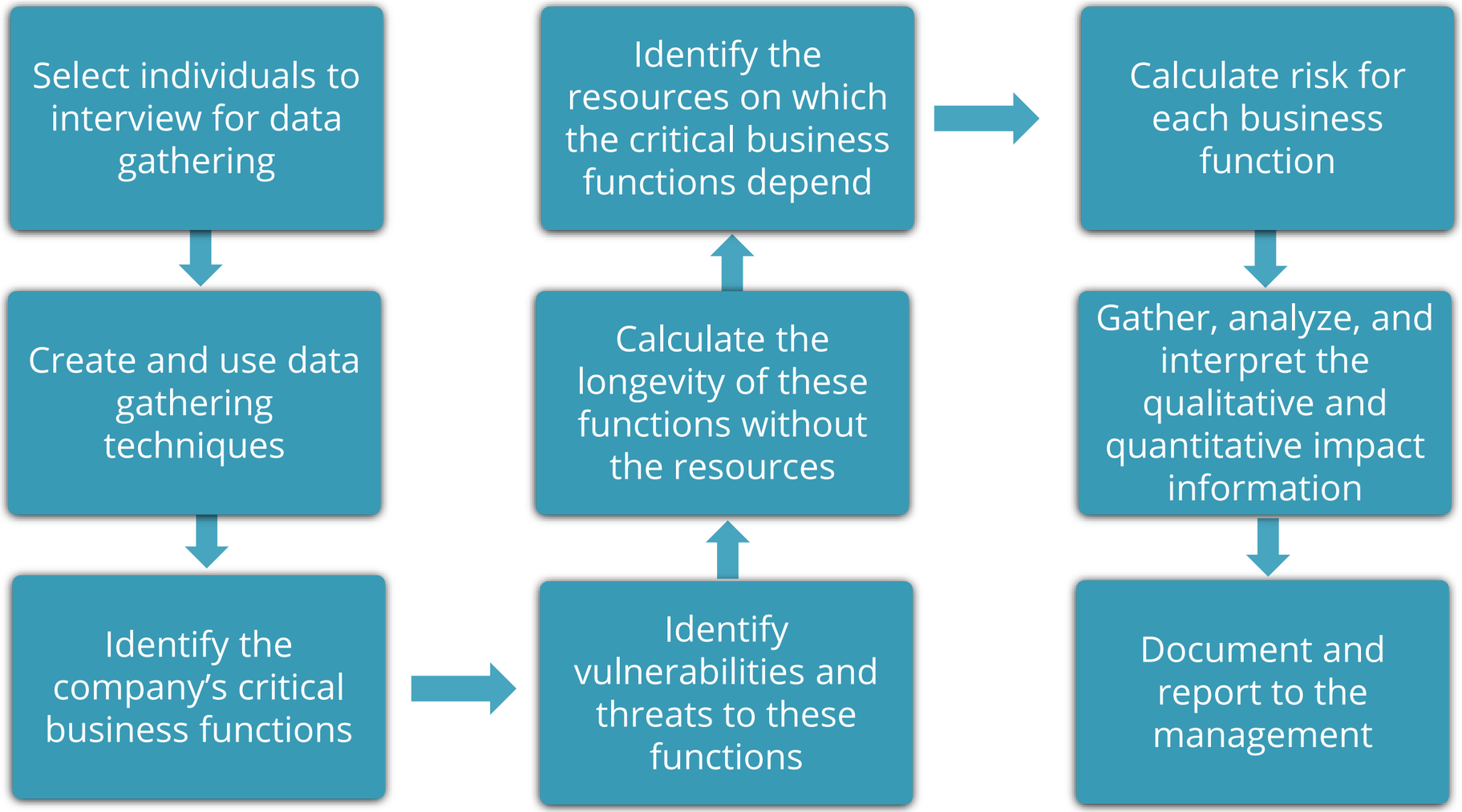
BIA: Goals

The three major goals of BIA are:

Criticality Prioritization	• Identification and prioritization of every critical business unit process • Evaluation of the impact of a disruptive event • Time-critical business processes require higher priority rating for recovery than non–critical business processes
Downtime Estimation	• Estimating Maximum Tolerable Downtime (MTD) using the BIA • The downtime required for the business to remain viable • Non-recovery, if the interruption of critical process extends the maximum tolerable downtime
Resource Requirements	• Estimating resource requirements • Most resources allocated to time sensitive processes as compared to less critical processes

BIA: Steps

The steps of a BIA are outlined here:



BIA Steps: Business Unit Level

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 required Maximum Tolerable Downtime (MTD)

Maximum Tolerable Downtime (MTD)

Maximum Tolerable Downtime (MTD) is:

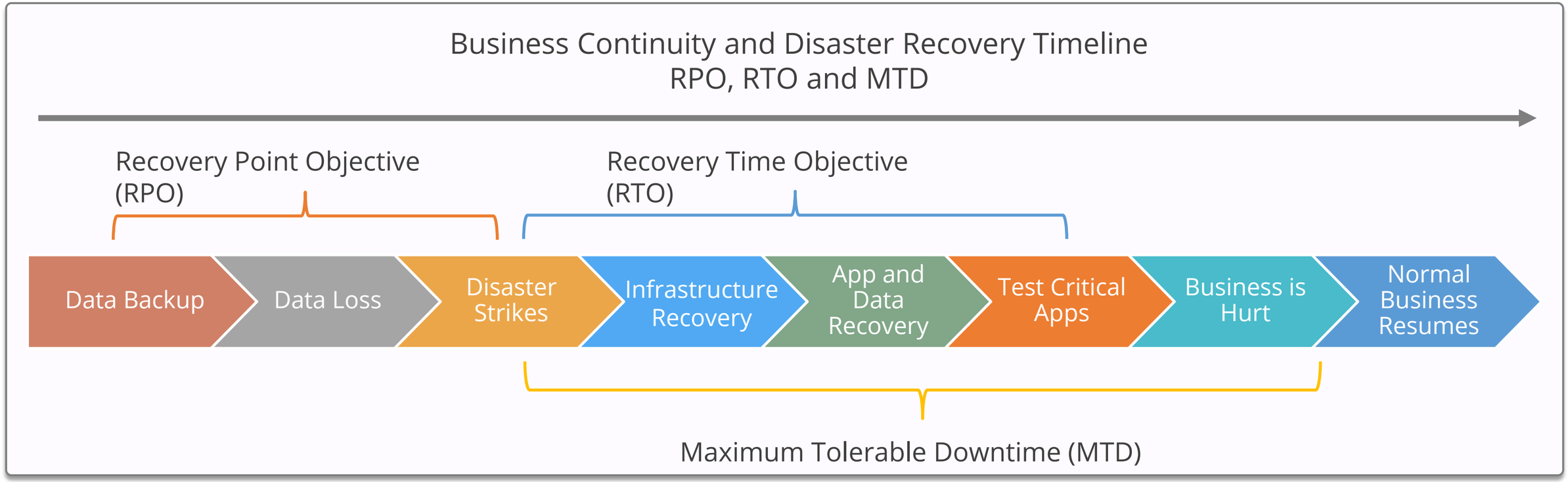
The maximum period for which the organization's key processes and functions are unavailable, after which the organization would suffer significant losses

Measured in minutes, hours, days, or longer, depending on the nature of the business

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

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

Work Recovery Time

- The 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

- The 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

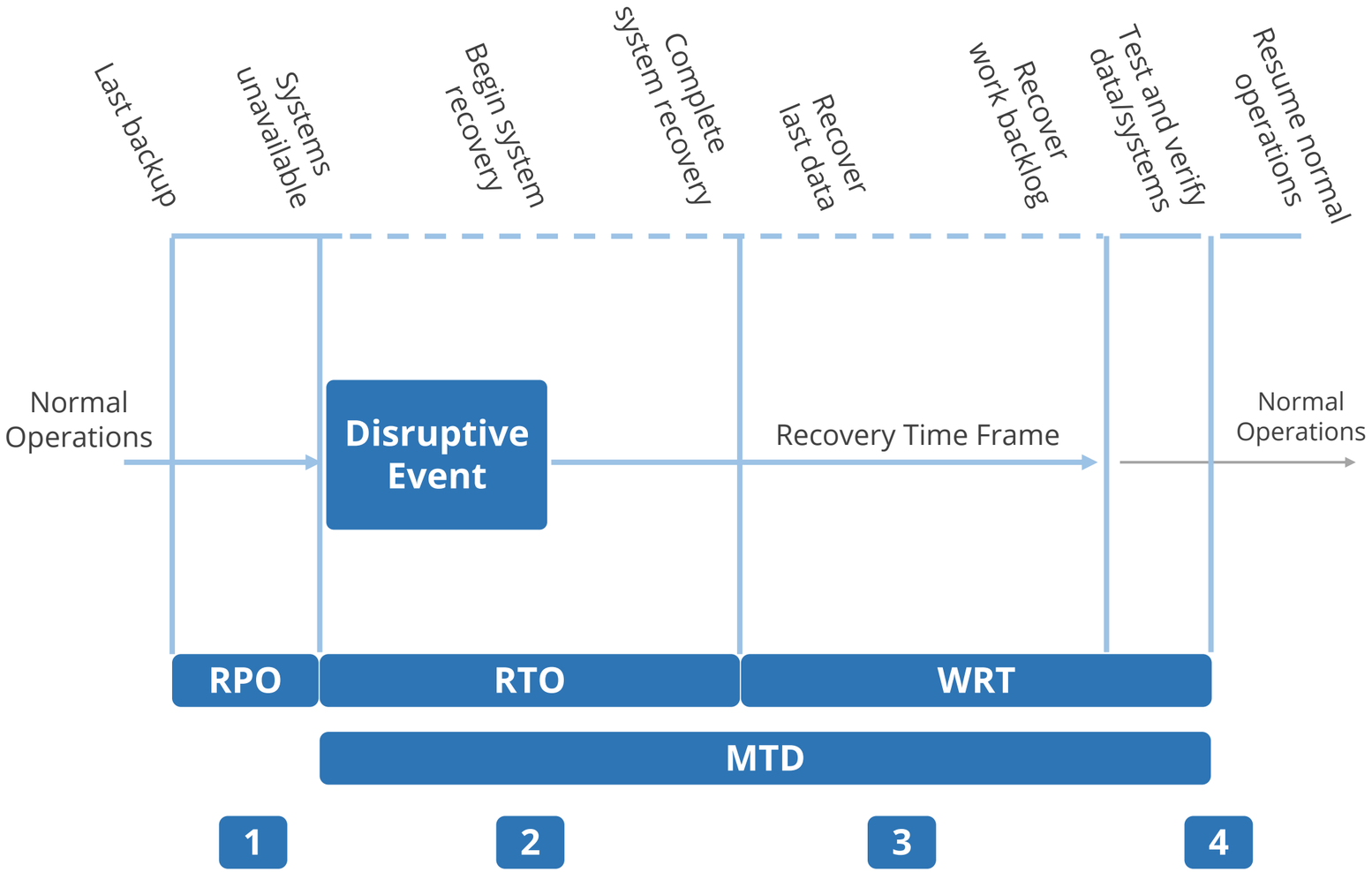
- The duration to recover a specific failed system
- The total corrective maintenance time divided by the total number of corrective maintenance actions during a given period

Minimum Operating Requirements

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

Stages of Failure and Recovery

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



BCP or DRP Phase 3: Identify Preventive Controls

According to NIST 800-34, Identify Preventive Controls is the third phase to achieve a comprehensive BCP or DRP. Preventive controls avert the potential impact of disruptive events.

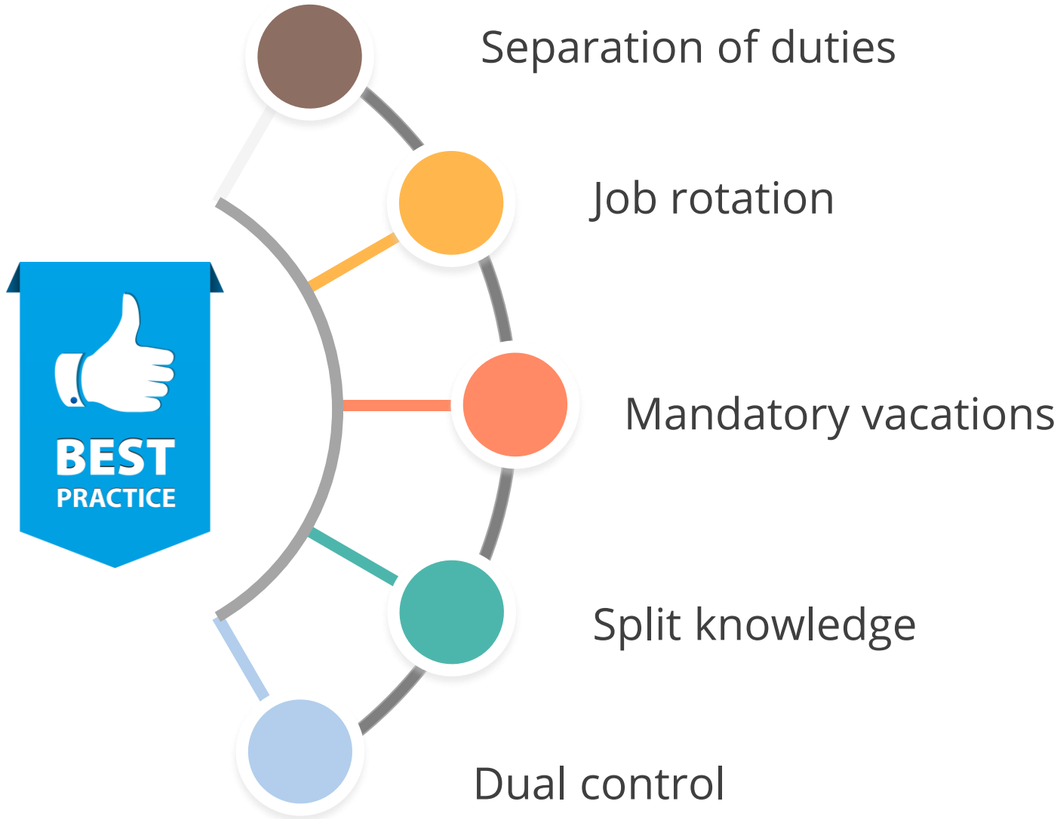
The types of preventive controls include:

Existing controls	Process or device that mitigates effect of a threat but cannot prevent occurrence
Physical controls	Fire suppression or sprinkler systems, access control systems, security guards
Procedural controls	Hiring and termination policies and clean desk policy
Logical controls	Data storage protection and protection given to assets based on their location

Contribute to and Enforce Personnel Security Policies and Procedures

Best Work Practices

Following are the best practices:



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 lifecycle 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

Managing Personnel Security: Hiring Practices

Following are the hiring practices:

- Perform background checks: Education, prior employment, financial history, and criminal history
- Get the confidentiality agreements signed: Non-Disclosure Agreement and Intellectual Property Agreement
- 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

Following are the employee termination policies:

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

Vendor, Contractors, and Consultant Controls

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.

Compliance: Need for Compliance

Compliance means conforming to a rule, such as a specification, policy, standard, or law.

Need for Compliance

- Protect critical information
- Enforce controls through formal written policy
- Understand the requirements for protecting organizational information
- Identify requirements for protecting organizational information
- Avoid inadequate implementation and enforcement; this can lead to fines, penalties, and imprisonment
- Avoid failures that lead to loss of customer confidence, competitive advantage, contracts, and jobs
- Protect shareholder interests
- Use good controls that make good business sense

Compliance Policy Requirements

Compliance policy facilitates compliance with applicable laws, regulations, policies, and standards.

Compliance training must be provided to all employees to ensure they are aware of their compliance responsibilities. Then training should be tailored to specific employees in high-risk areas.

Audits are performed to ensure compliance to contracts, regulations, and laws and assist in detecting abnormal activities.

Acceptable Usage Policy

- Outlines which activities are acceptable and unacceptable 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 non-compliance 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 minimum, an organization’s privacy policy should disclose what personal or sensitive information they collect, how they collected it, how they intend to use that information, and whether they will disclose some or all the information to any third parties.

Understand and Apply Risk Management Concepts

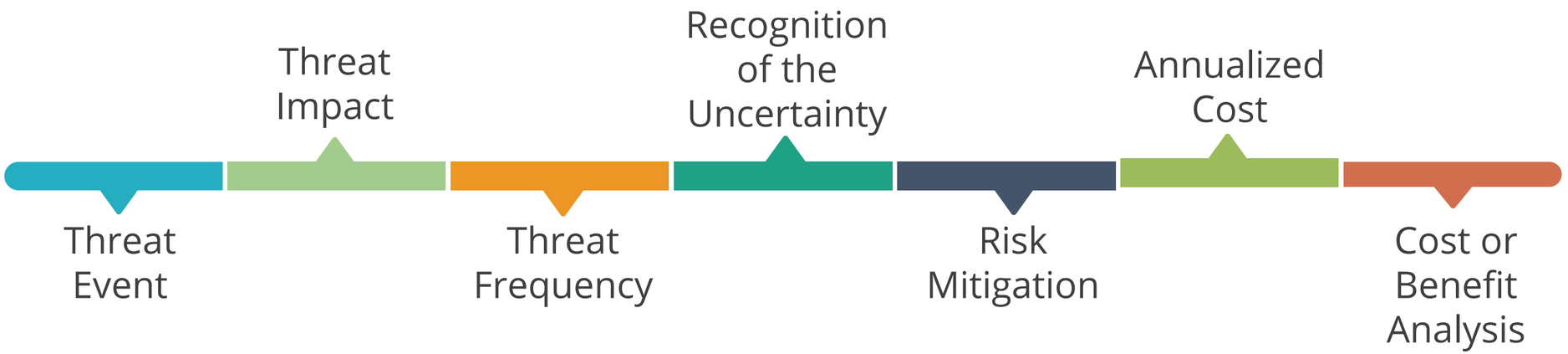
Security Definitions

A few security terms that a CISSP candidate must know:

1. **Asset:** An asset is any information, software, hardware, or equipment that is utilized for, and critical to, business objective, service delivery, and financial success.
2. **Vulnerability:** Vulnerability is any hardware, software, or procedural weakness that may give an attacker the open door for unauthorized access to resources.
3. **Threat:** Threat is any potential danger to systems or information.
4. **Threat Agent:** Threat agent is any entity that takes advantage of a vulnerability.
5. **Risk:** Risk is the likelihood of a threat agent taking advantage of a weakness or vulnerability and the resulting business impact.
6. **Exposure:** Exposure is an instance of being exposed to losses from a threat agent.
7. **Countermeasure or Safeguard**: Countermeasure or safeguard is put into place to mitigate the potential risk.

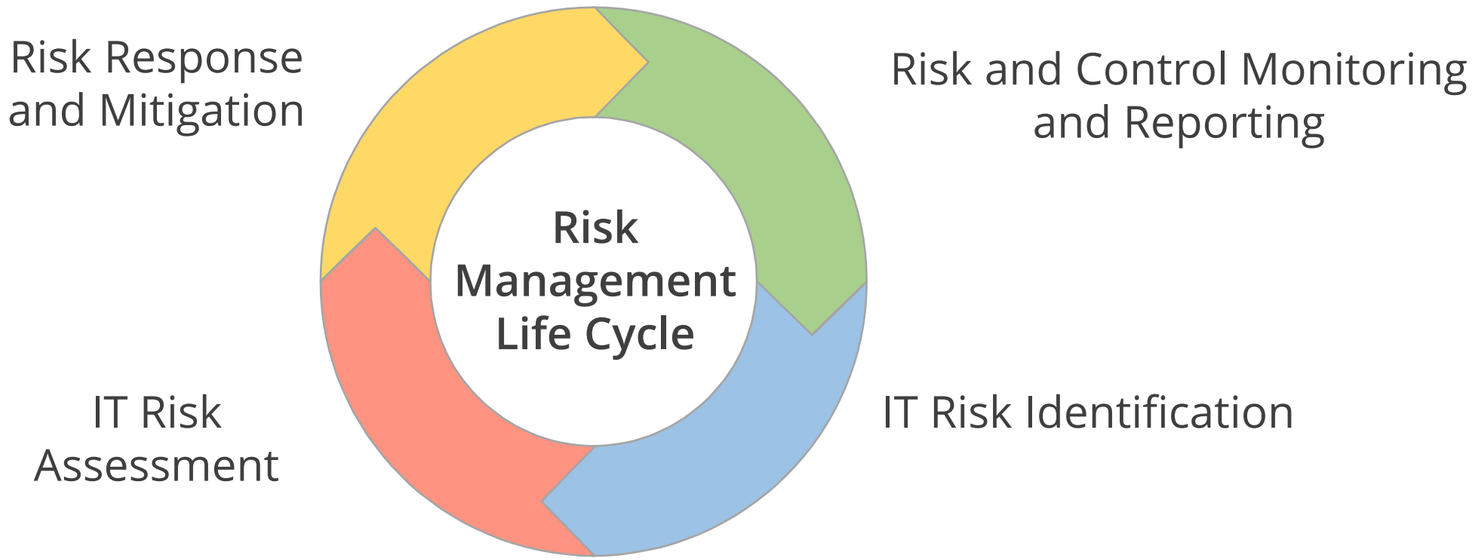
Information Risk Management

Information Risk Management 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:



Business Scenario

While studying the Information Risk Management process, Kevin made notes on the security definitions based on examples from his day-to-day work:

- Asset: Servers and systems of the company
- Vulnerability: Weak rule in firewall
- Threat: Hacking network or servers
- Threat Agent: Hacker
- Risk: Loss of critical organization data
- Exposure: 25% loss of data (which is unencrypted)

Question: What will the risk management process achieve?

Business Scenario

While studying the Information Risk Management process, Kevin made notes on the security definitions based on examples from his day-to-day work:

- Asset: Servers and systems of the company
- Vulnerability: Weak rule in firewall
- Threat: Hacking network or servers
- Threat Agent: Hacker
- Risk: Loss of critical organization data
- Exposure: 25% loss of data (which is unencrypted)

Question: What will the risk management process achieve?

Answer: It helps to maintain the identified risks at an acceptable level.

Introduction to Risk Analysis

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

- Risk analysis prioritizes risks and calculates the cost of safeguards.
- It provides a cost/benefit comparison between cost of safeguards and 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

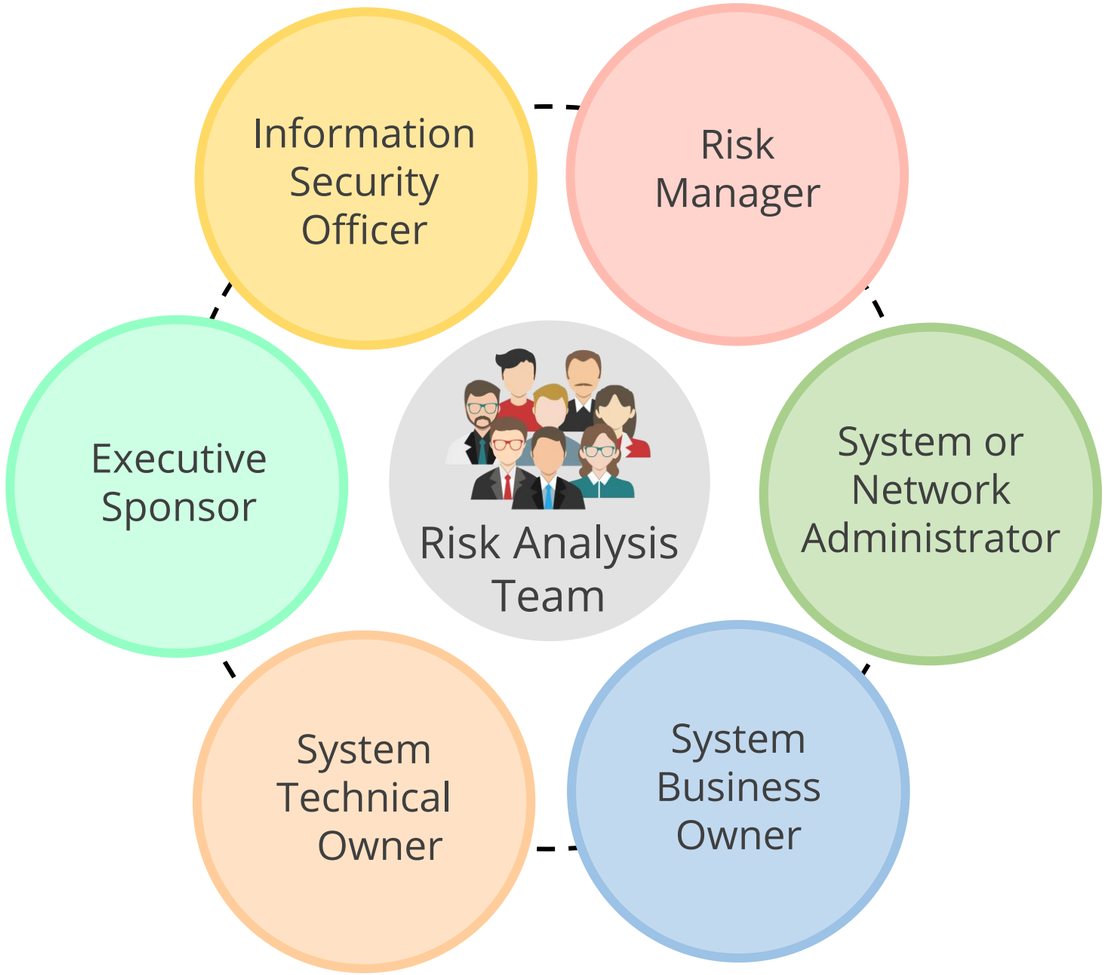
To identify vulnerabilities and threats

To balance the cost of countermeasure and the impact of threats

To measure probability and the impact of latent threats

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 Team

The steps to perform risk analysis:

Risk analysis and assessment

Asset and information value assignment

Countermeasure selection and implementation

Information and Asset 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

Information and Asset Valuation

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

- 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

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

Key Terms in Quantitative Risk Analysis

Asset	• Total value of assets
Exposure Factor	• 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 • It is calculated in dollars

Key Terms in Quantitative Risk Analysis

Annualized Rate of Occurrence (ARO)

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

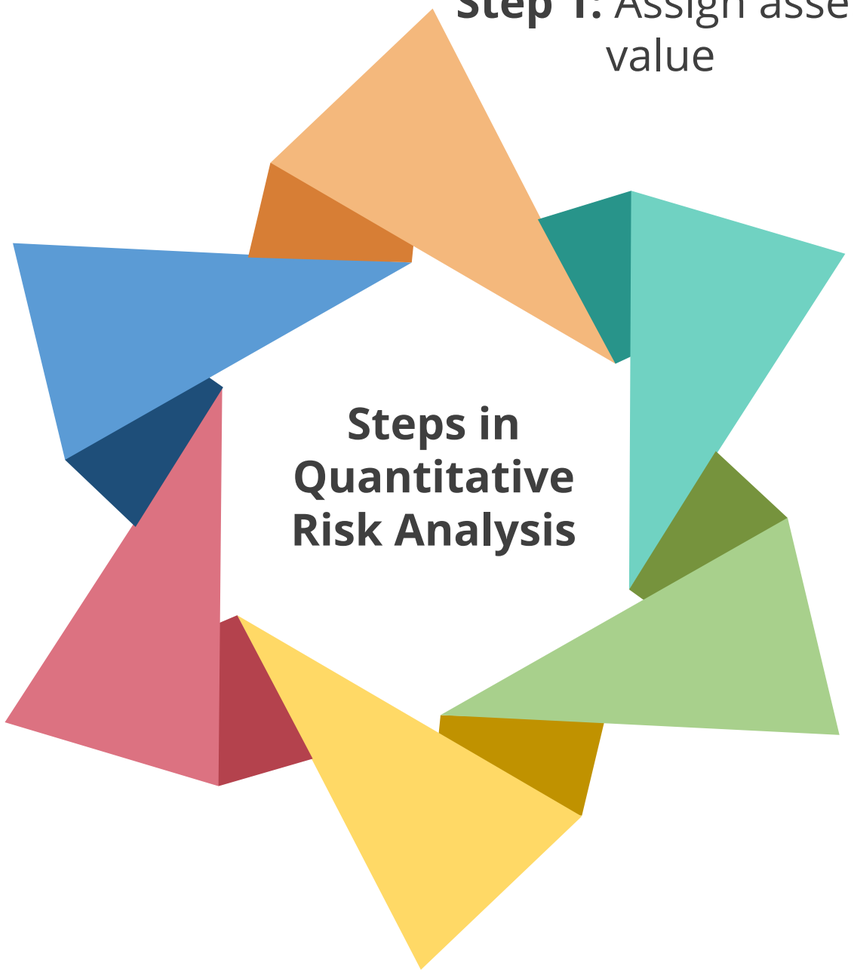
Annualized Loss Expectancy (ALE)

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

Annual Cost of Safeguard (ACS)

- The cost associated in procuring, developing, and maintaining control against a potential threat
- The ACS 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 or 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. Examples of qualitative techniques to gather data are:

- 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, 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

Hybrid analysis 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.

Countermeasure Selection: 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

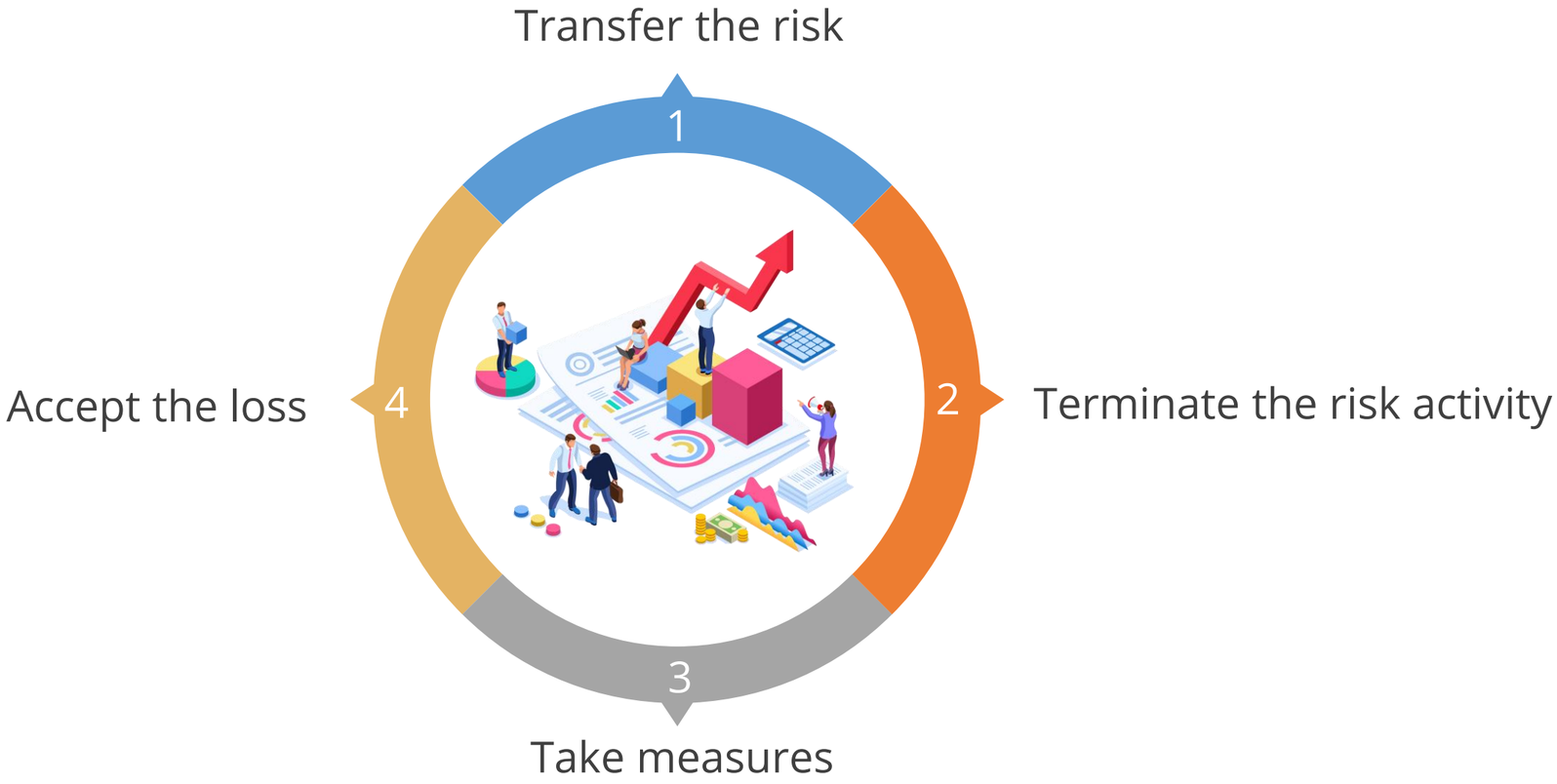
Countermeasure Selection: Other Factors

Other factors that influence the selection of countermeasure or safeguard:

Total Cost of Ownership (TCO)	TCO is the total cost of a mitigating safeguard
Return on Investment (ROI)	ROI is the amount of money saved by implementing a safeguard
Uncertainty	Uncertainty refers to the degree to which you lack confidence in an estimate. This is expressed as a percentage, from 0 to 100 percent. If you have a 25 percent confidence level in something, then it could be said that you have a 75 percent uncertainty level.

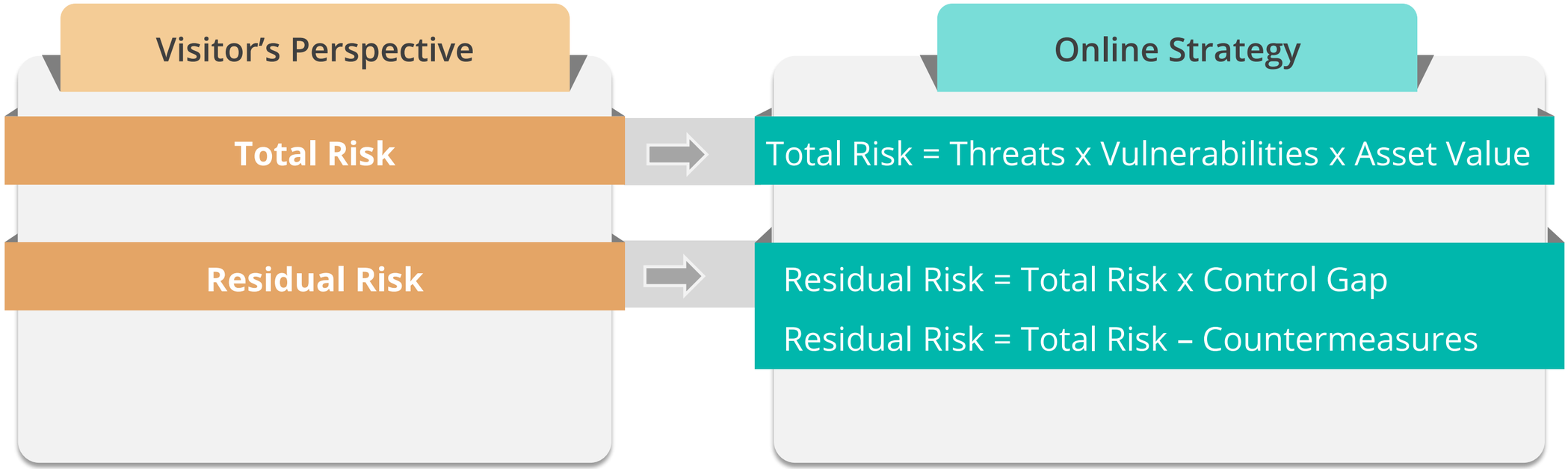
Handling Risk

Risk treatment can be done in the following four ways:



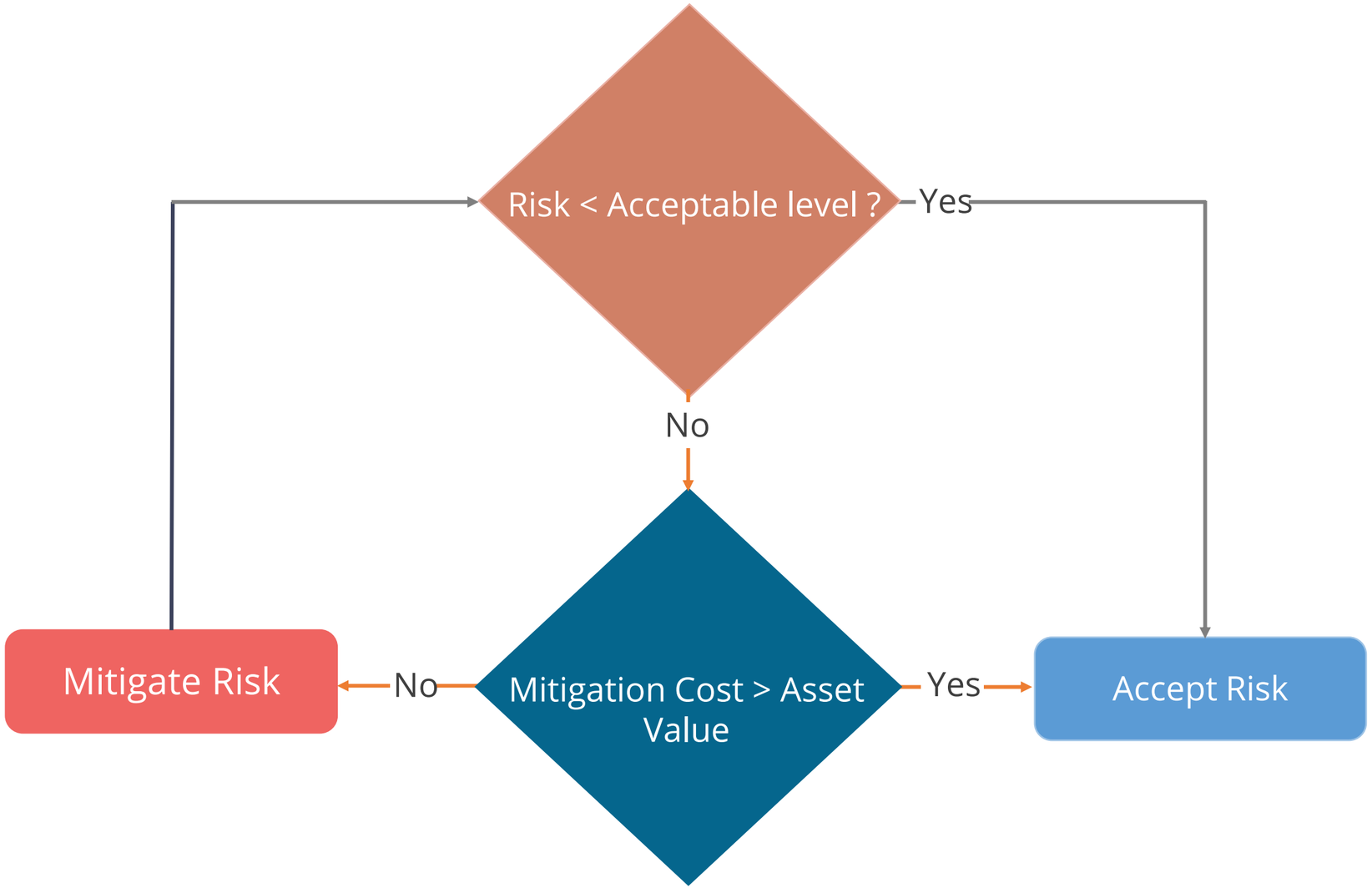
Handling Risk

Conceptual formulas to calculate total risk and residual risk:



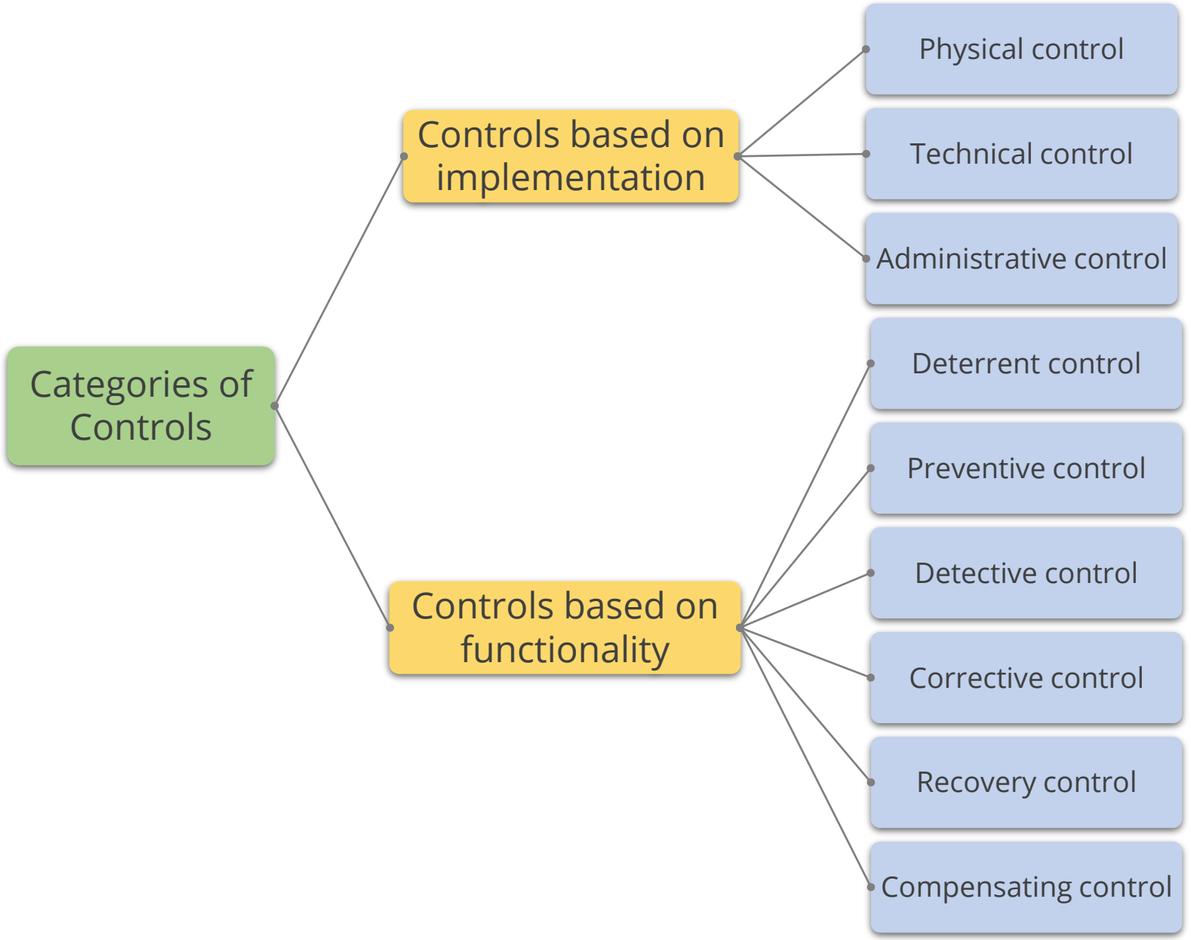
Residual Risk Mitigation

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



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

- They are commonly referred to as soft controls because they are more management oriented.
- Examples of administrative controls are security documentation, risk management, personnel security, and training

Technical controls

- Technical controls, also called logical controls, are software or hardware components.
- Examples: Firewalls, IDS, encryption, identification, and authentication mechanisms

Physical controls

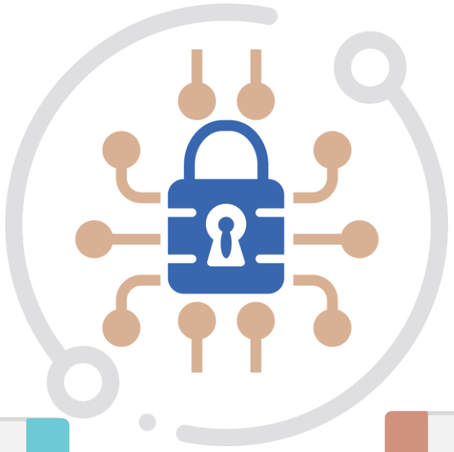
- They are items put into place to protect facility, personnel, and resources.
- Examples of physical controls are security guards, locks, and fencing

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)



Security control assessment (SCA) 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.

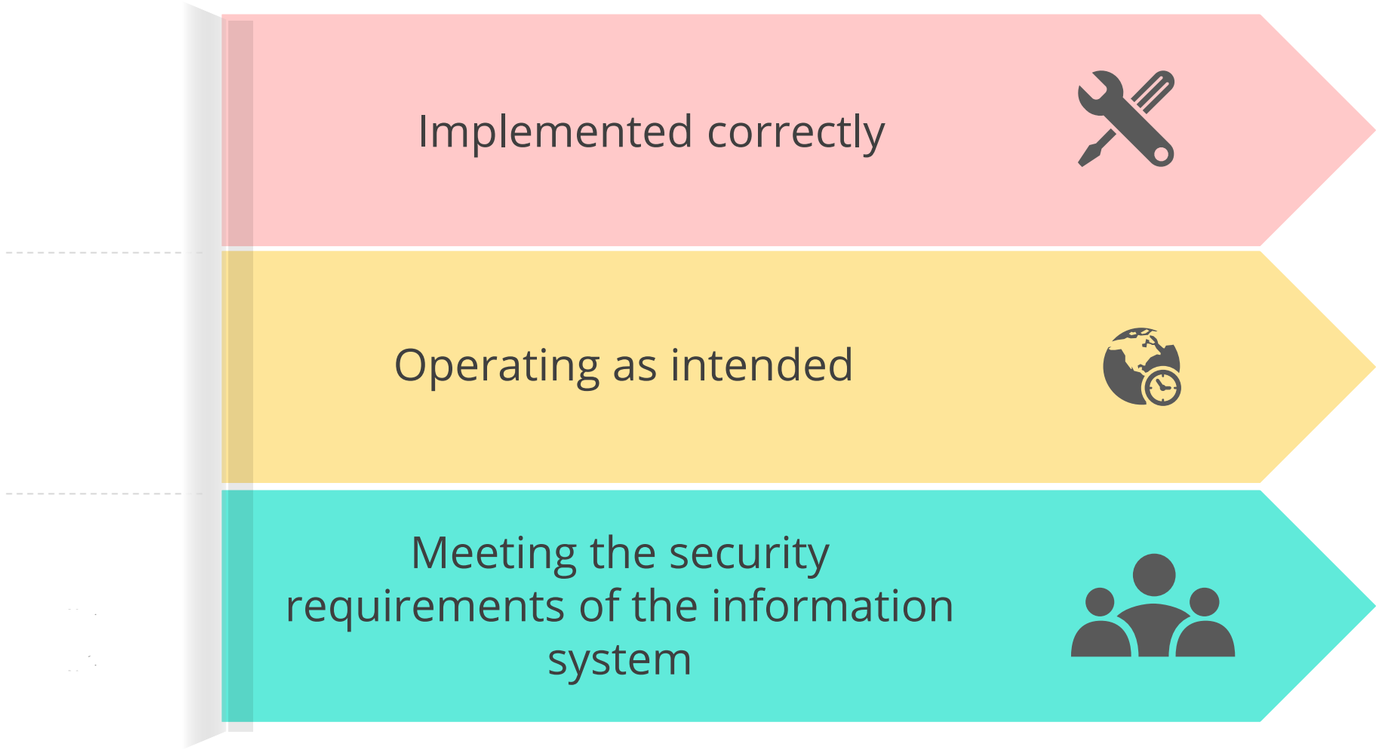
Security Control Assessment (SCA)

SCA results provide:

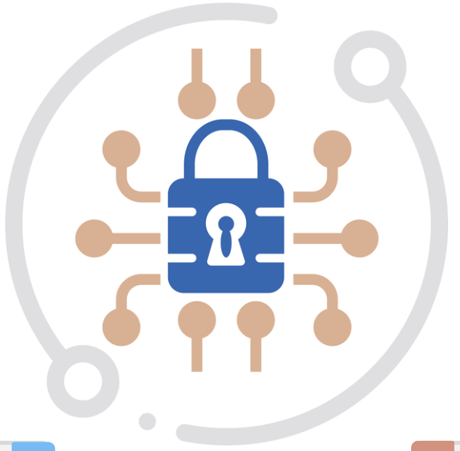
- Evidence of the effectiveness of implemented controls
- An indication of the quality of the risk management processes employed within the organization
- Information about the strengths and weaknesses of information systems that are supporting organizational missions and business functions

Assurance for Security Control Effectiveness

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



Security Control Assessment (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 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.
- Common controls utilized for high and moderate impact systems must be performed by an independent assessment team.
- They prepare the final security assessment report containing the results and findings of the assessment.

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 relevant stakeholders in order to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

Risk Measurement

KRIs and KPIs can be used to measure, monitor, and report risk. The two are explained below in detail.

Key risk indicator (KRI)

- A key risk indicator (KRI) is a measure used in risk management to indicate how risky an activity is.
- By comparing an appropriate set of key risk indicators with defined thresholds, organizations receive an early warning when a risk approaches an unacceptable level.

Key performance indicators (KPIs)

- A key performance indicator (KPI) is used to measure how well a process is performing in terms of its stated goal.
- KPIs 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.

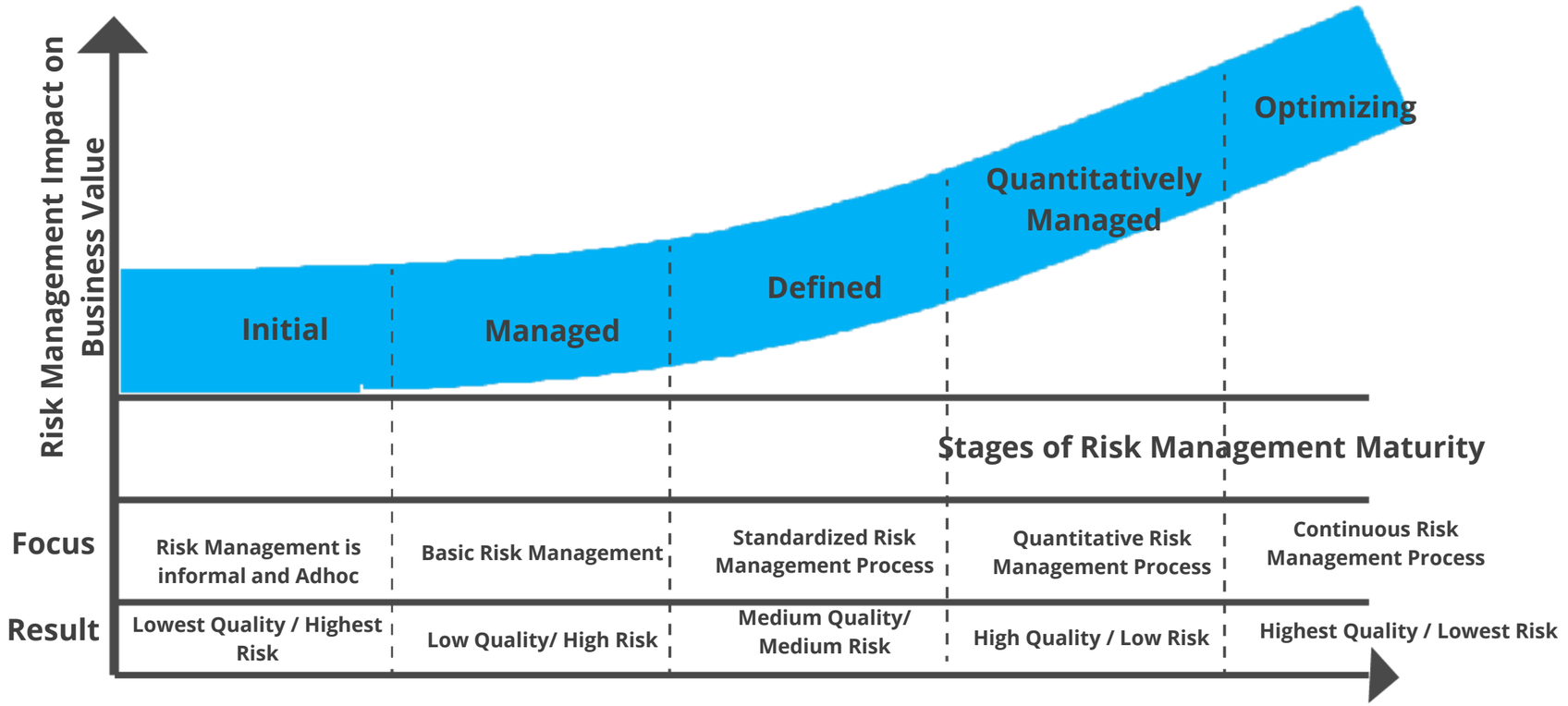
Continuous Improvement

Organizations can use a risk maturity model to improve their risk management processes by identifying their current and desired capabilities.

A mature risk management program is better at preventing, detecting, and responding to security incidents.

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

Continuous Improvement



Risk Frameworks

Risk management framework is used to identify, measure, manage, monitor, and report the significant risks to the achievement of business objectives.

There are three risk frameworks, namely:

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

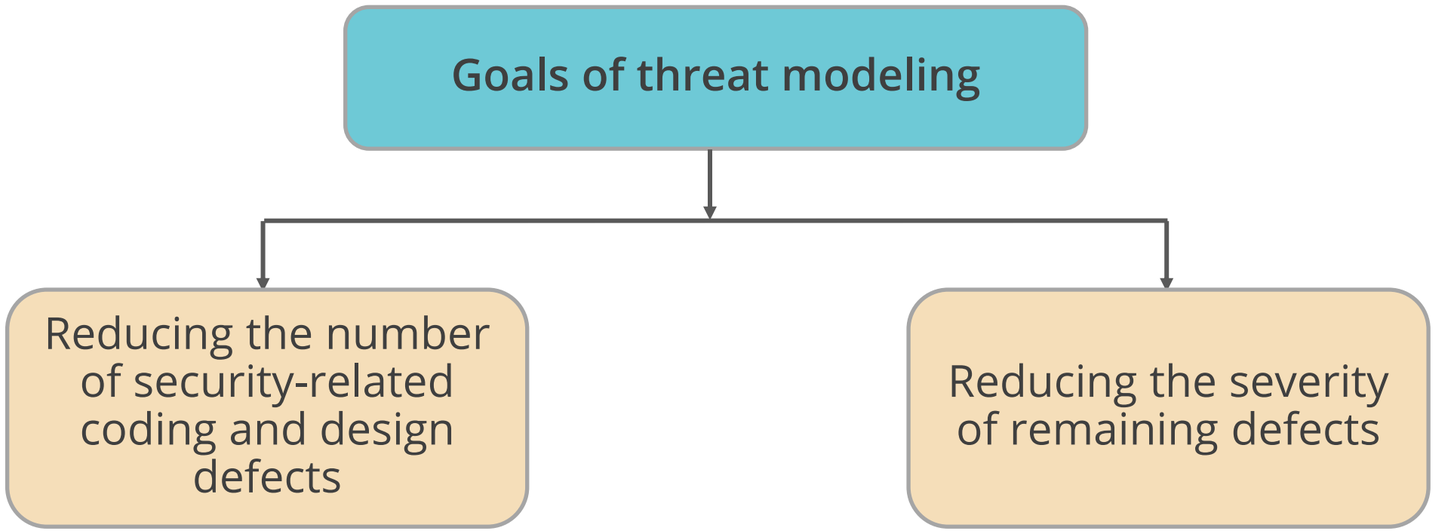
Understand and Apply Threat Modeling Concepts and Methodologies

Threat Modeling

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

Threat Modeling



Threat Modeling

Approaches to threat modeling:

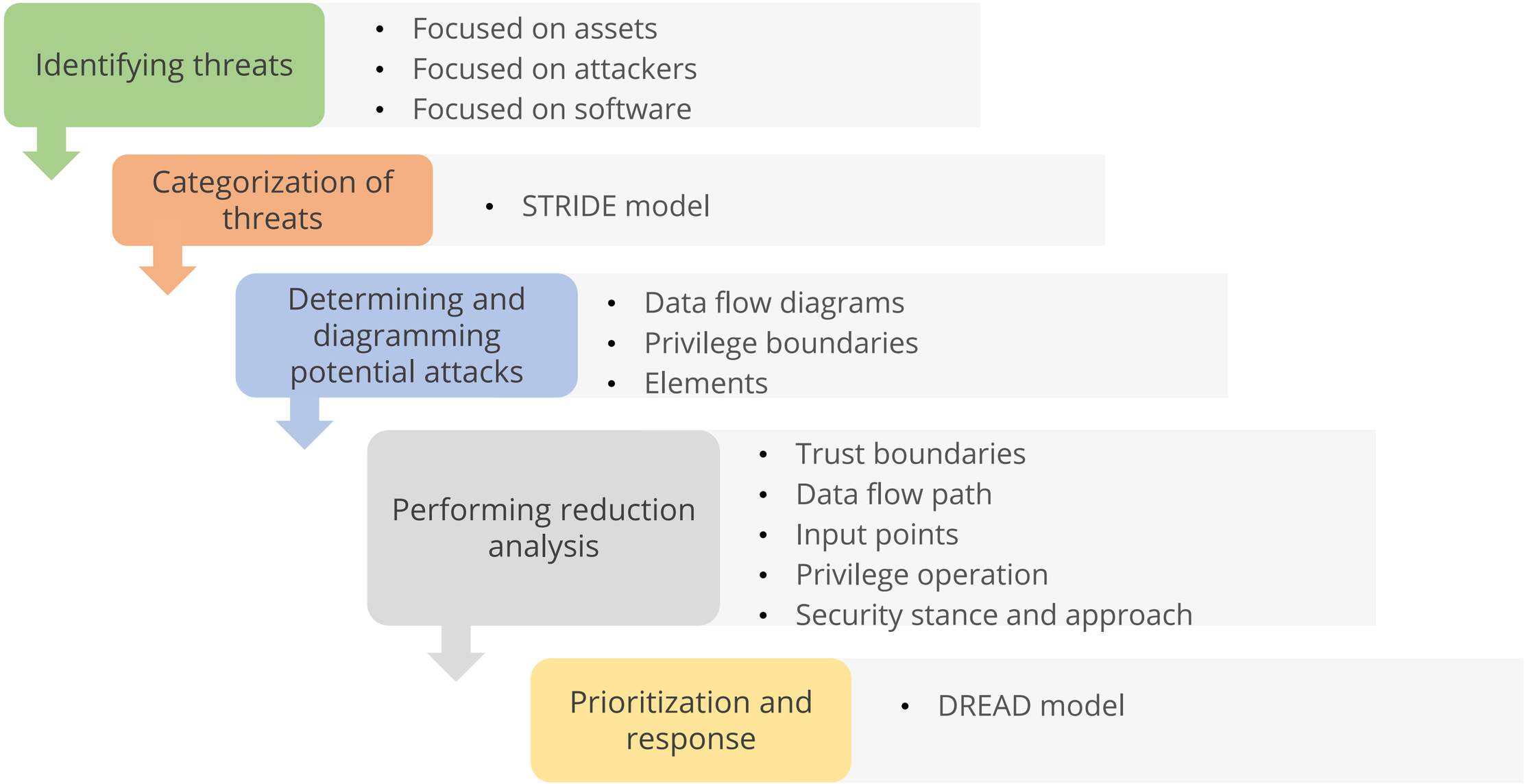
Proactive Approach

- 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
- This is the core concept behind ethical hacking, PT, source code review, and fuzz testing

Threat Modeling Steps



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)

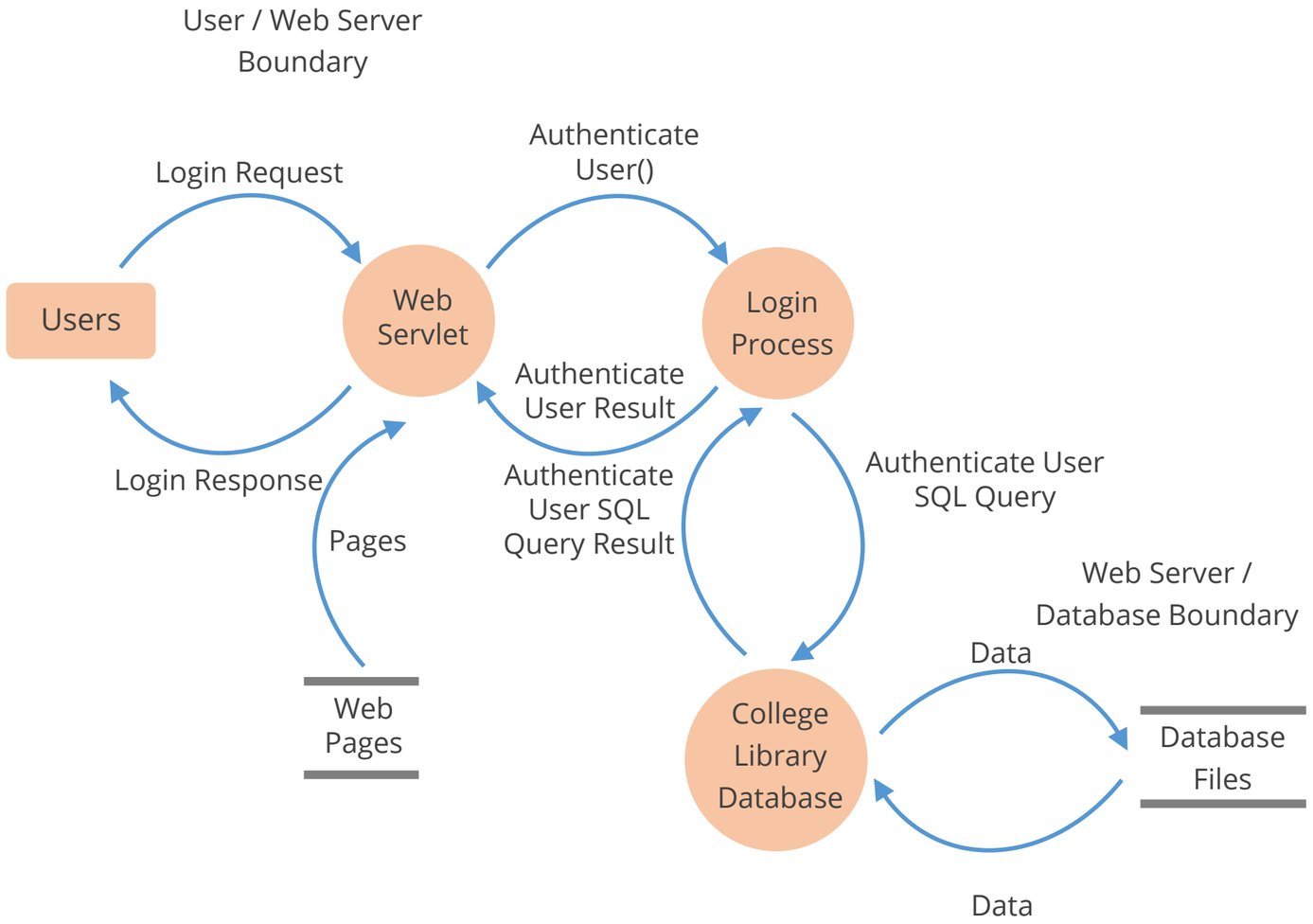
Spoofing	An attack with the goal of gaining access to a target system through the use of a falsified identity
Tampering	This is used to falsify communications or alter static information
Repudiation	The ability of a user or an attacker to deny having performed an action or activity
Information disclosure	The revelation or distribution of private, confidential, or controlled information to external or unauthorized entities
Denial of service (DoS)	An attack that attempts to prevent an authorized use of a resource
Elevation of privilege	An attack where a limited user account is transformed into an account with greater privileges, powers, and access

Step 3: Determining and Diagramming Potential Attacks

Determining and Diagramming Potential Attacks

- Post identifying threats, the next step is to determine the potential attack concepts that could materialize
- Often accomplished by data flow diagrams, privilege boundaries, and elements involved
- Once a diagram has been crafted, identify all the technologies involved
- Identify attacks that could be targeted at each element of the diagram
- Attacks should include all forms: logical, physical, and social

Step 3: Determining and Diagramming Potential Attacks



Step 4: Performing Reduction Analysis

Reduction analysis involves decomposing the application, system, or environment.

Input points
Locations where an external input is received

Data flow paths
Movement of data between locations

Privilege operations
Activities that require greater privileges

Trust boundaries
Locations where the level of trust changes

Security stance and approach
Declaration of the security policy, security foundation, and security assumptions

Step 5: Prioritization and Response

Prioritization and Response

- Rates the threats in order 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

DREAD rating system:

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
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

Threat description	Injection of SQL commands
Threat target	Data access component
Risk rating	
Attack techniques	Attacker appends SQL commands to username, which is used to form 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

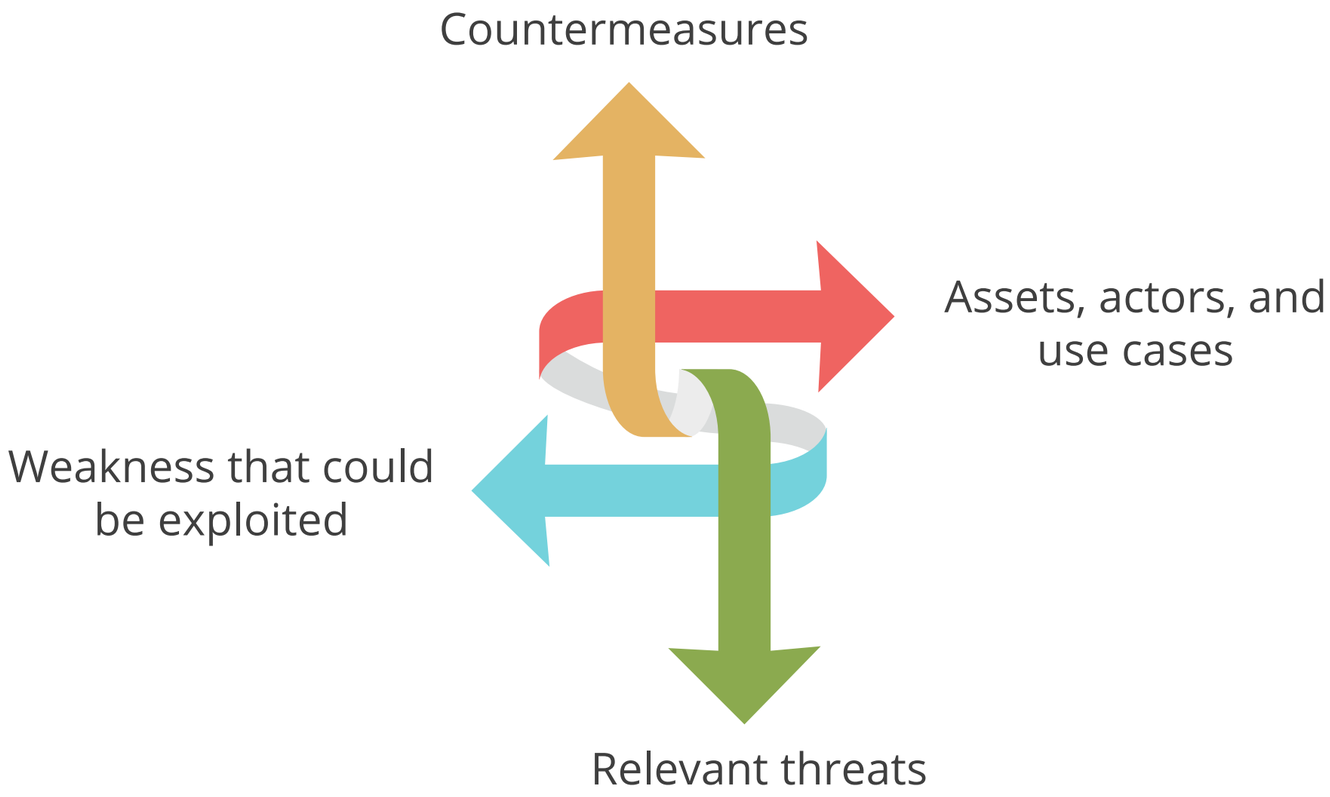
Threat description	Attacker obtains authentication credentials by monitoring the network
Threat target	User authentication process in a web application
Risk rating	High
Attack techniques	Attacker uses network monitoring software
Countermeasures	Use SSL to provide an encrypted channel

Threat Template

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

Threat Modeling Outcomes

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



Apply Supply Chain Risk Management (SCRM) Concepts

Supply-Chain Risk Management

Supply chain is the network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product, from the delivery of source materials from the supplier to the manufacturer through to its eventual delivery to the end user.

Supply-chain risk management (SCRM) is a process to help identify, monitor, detect, and mitigate threats to supply chain continuity and profitability.

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

It 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 lifecycle 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

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 between a company and another entity, by contract or otherwise.
- Outsourcing is the subcontracting of a business process to a third-party company.
- Organizations are increasingly outsourcing systems, business processes, and data processing to service providers in an effort to focus on core competencies, reduce costs, and more quickly deploy new application functionality.
- Third-party risk management is a comprehensive plan for identifying and mitigating potential business uncertainties and legal liabilities regarding the hiring of third-party services.

Third-Party Risks

Information Security or Data Privacy

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

Third party cannot continuously maintain its services due to business disruption (e.g., ineffective redundancy procedures).

Financial Viability

Third party is not financially secure to continue to provide you services at acceptable levels.

Third-Party Risks

Contract Compliance

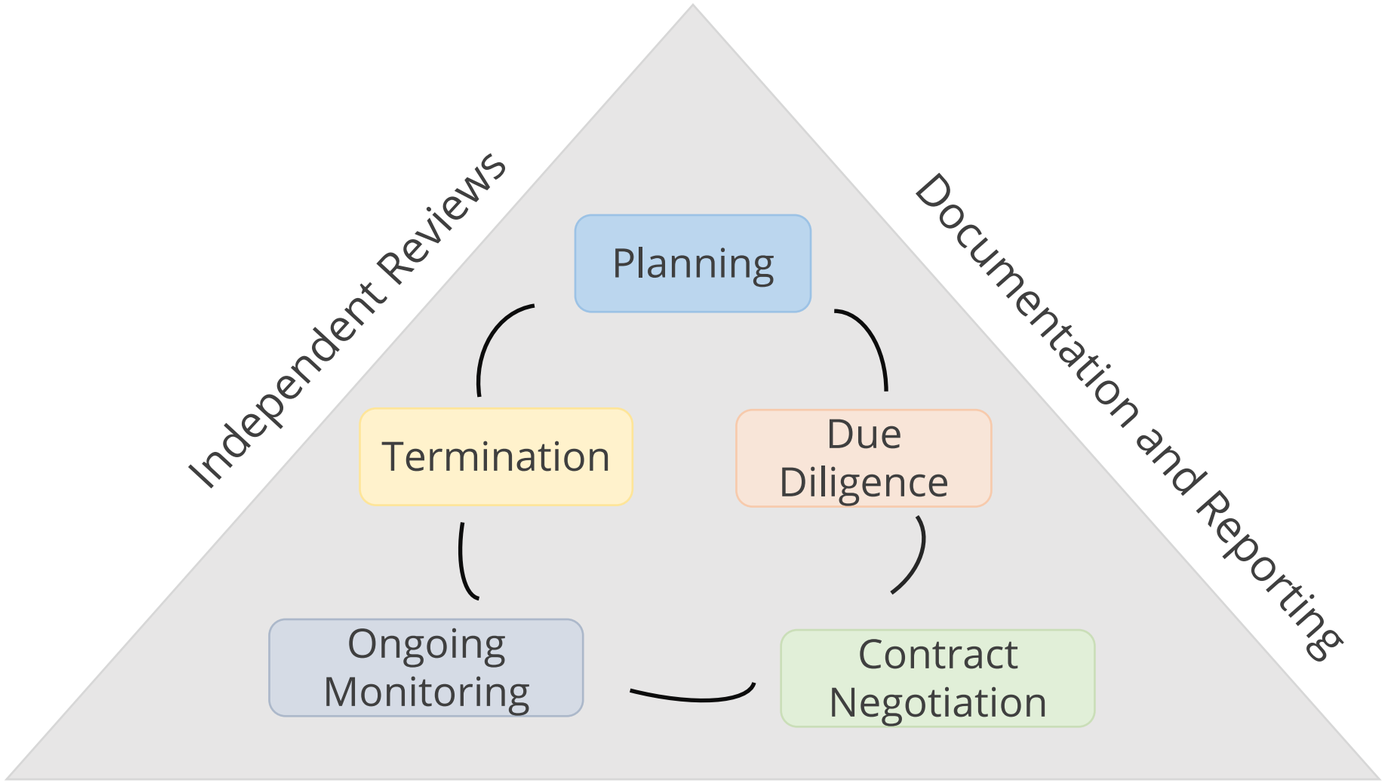
Third party products, services, or systems are not consistent with your policies and procedures, applicable laws, regulations, and ethical standards.

Legal or Regulatory

Third party does not possess the necessary licenses to operate. It lacks the expertise to enable the company to remain compliant with domestic and international laws and regulations.

Third-Party Risk Management

The diagram given below will help us to understand the third-party risk management.



Third-Party Risk Management

The plan should oversee the full lifecycle of a third-party relationship including:

- 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 that outline the rights and responsibilities of all parties
- Ongoing monitoring of the third party’s activities and performance
- Contingency plans for terminating the relationship in an effective manner
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process
- Documentation and reporting that facilitate oversight, accountability, monitoring, and risk management
- Independent reviews that allow organization's management to determine that processes align with its strategy and effectively manage risks

Third-Party Risk Management Lifecycle

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 Lifecycle

Conduct a review of a potential third party before signing a contract to ensure that the organization selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the organization's risk appetite. On-site visits may be useful to fully understand the third party's 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 Lifecycle

Develop a written contract that clearly defines expectations and responsibilities of the third party to ensure the contract's enforceability, limit the organization's liability, and mitigate disputes about performance.

- 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 entering into a contract with a third party, organization management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party's 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

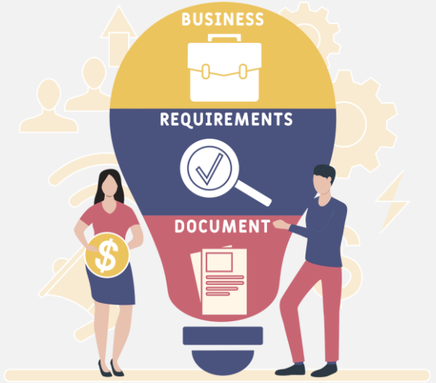
A contingency plan need to be developed to ensure that the organization can transition the activities to another third party. Termination can happen for bringing the activities in-house, or discontinuing the activities when a contract expires, when the terms of the contract have been satisfied, in response to contract default, or changes to the organization's or third party's 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 the security functionality in a proposed product does not satisfy specific security requirements, then the risk introduced must be evaluated and additional controls must be reconsidered prior to purchasing the product.
- When additional functionality is supplied and causes a security risk, it must be disabled or the proposed control structure must be reviewed to determine if advantage can be taken of the available enhanced functionality.

Service-Level Requirements



A Service-Level Requirements (SRL) document 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 Service-Level Requirements (SRL).

Real World Scenario

In 2017, Verizon, a major telecommunications provider, suffered a data security breach with over 14 million US customers' personal details exposed on the internet after Nice Systems, a third-party vendor, mistakenly left the sensitive users' details open on a server.

- Verizon's partner Nice Systems logged customer files that contained sensitive and personal information (including customer names, corresponding cell phone numbers, and specific account PINs) on an Amazon S3 bucket.
- For reasons unknown, that bucket was left unsecured, thus exposing more than 14 million Verizon customer records to anyone who discovered the bucket.

Question: Among Verizon, NICE Systems, and Amazon, who is accountable for the data loss?

Real World Scenario

In 2017, Verizon, a major telecommunications provider, suffered a data security breach with over 14 million US customers' personal details exposed on the internet after Nice Systems, a third-party vendor, mistakenly left the sensitive users' details open on a server.

- Verizon's partner Nice Systems logged customer files that contained sensitive and personal information (including customer names, corresponding cell phone numbers, and specific account PINs) on an Amazon S3 bucket.
- For reasons unknown, that bucket was left unsecured, thus exposing more than 14 million Verizon customer records to anyone who discovered the bucket.

Question: Among Verizon, NICE Systems, and Amazon, who is accountable for the data loss?

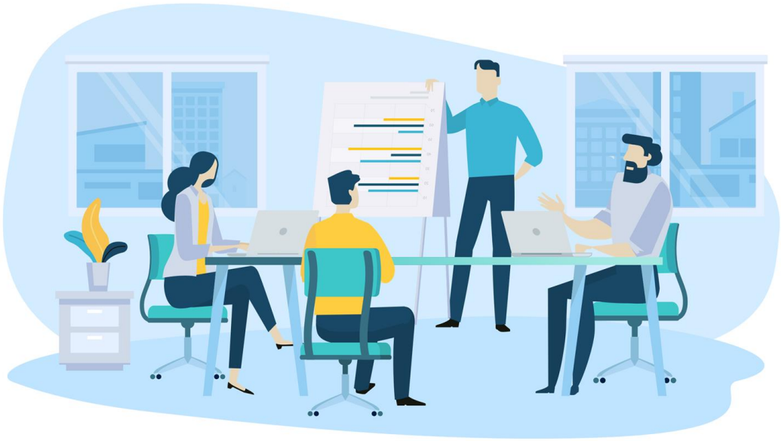
Answer: Verizon. They should have ensured visibility into how partners and other stakeholders keep their data secure.

Establish and Maintain a Security Awareness, Education, and Training Program

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: Awareness, Training, and Education

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

Methods and Techniques to Present Awareness and Training

Security awareness training could help organizations protect against **social engineering** attacks such as **phishing**.

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.

For example, a security champion within a software development team can help other developers prioritize security and improving the overall quality of the products.

Methods and Techniques to Present Awareness and Training

Security leaders can use **gamification** to enhance cyber security training for their employees.

Gamification is the use of game principles in nongame business scenarios by engaging and motivating people to achieve business outcomes.

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

Business Scenario

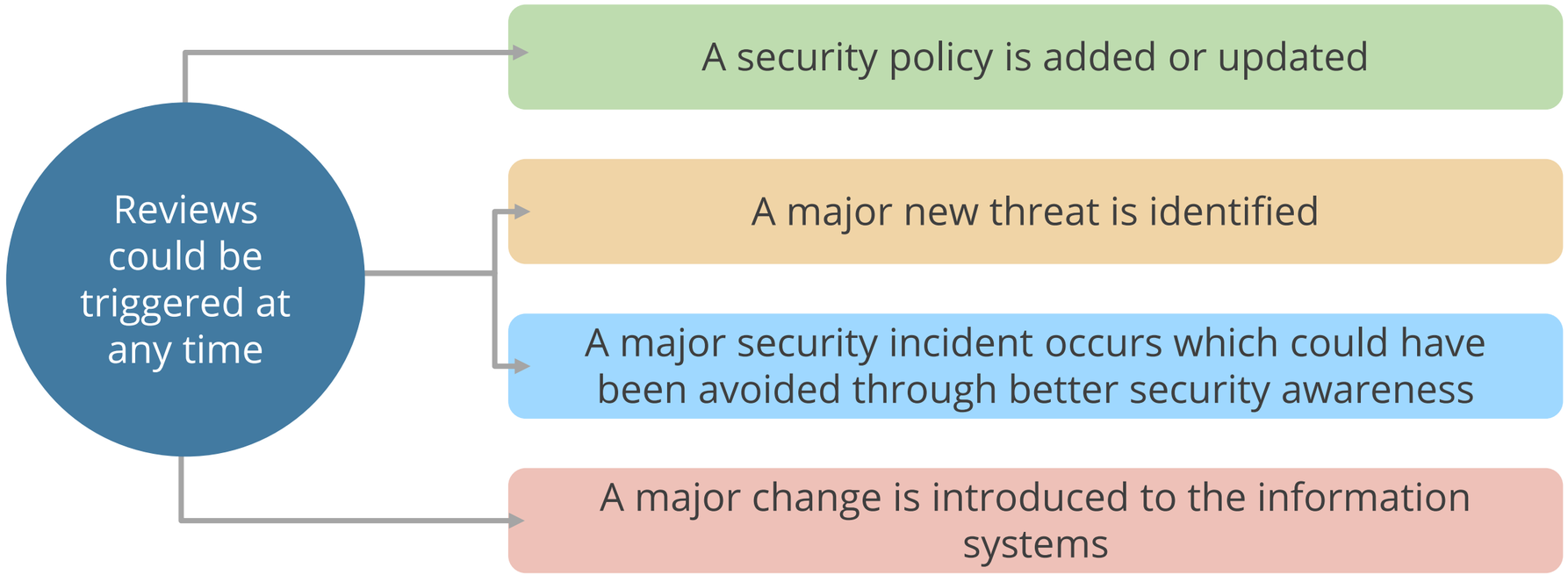
PwC launches Game of Threats

- 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 cyber attacks.
- 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.

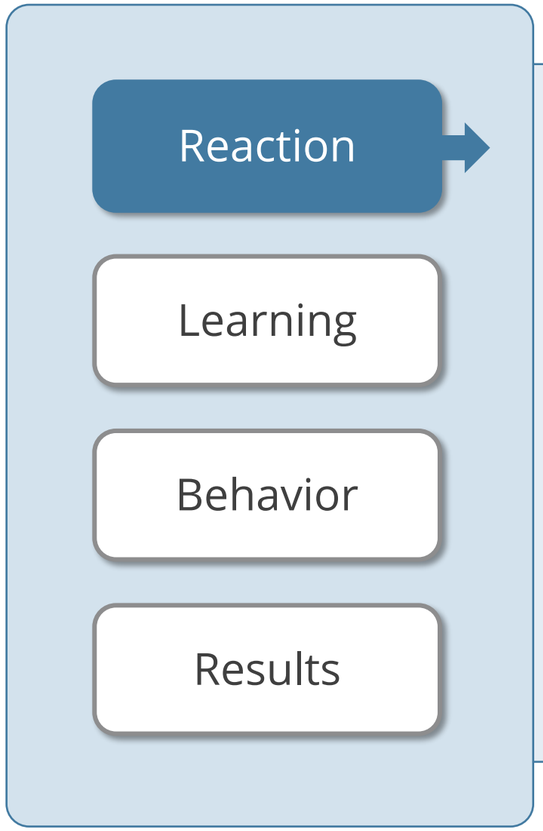
Information source: https://www.pwc.co.uk/issues/cyber-security-services/game-of-threats.html

Periodic Content Reviews

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



Program Effectiveness Evaluation

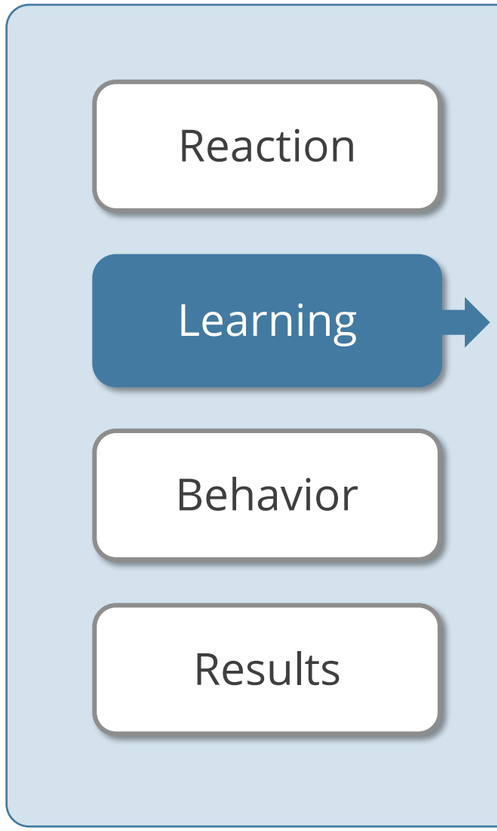


To what degree participants react favorably to the training

Sample questions to measure learning:

- 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?

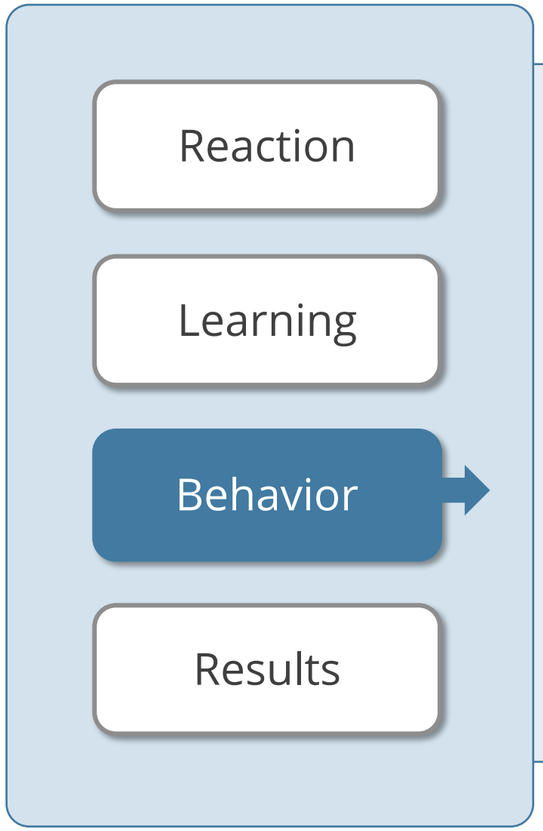
Program Effectiveness Evaluation



- 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?

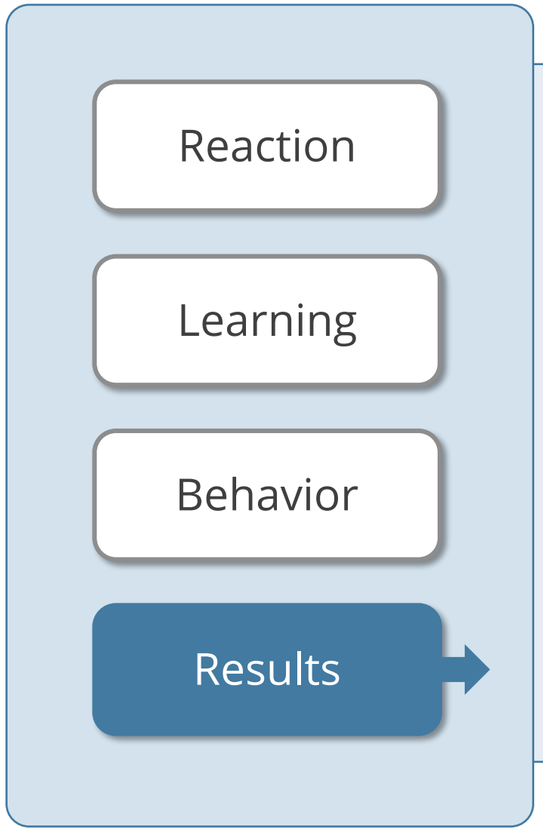
Program Effectiveness Evaluation



- 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've changed their behavior?

Program Effectiveness Evaluation

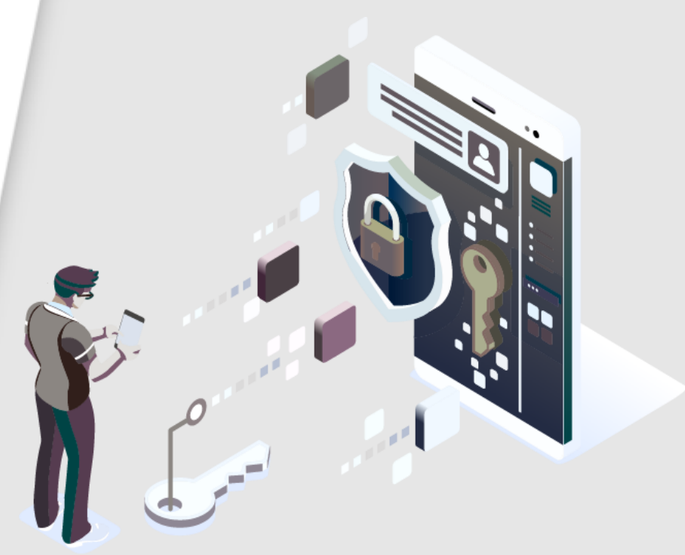


- To what degree targeted outcomes occur as a result of the training event and subsequent reinforcement

- **Sample key metrics to measure results:**
  - Improved work quality and productivity
  - Improved business results (e.g., sales, customer satisfaction, and retention)
  - Increased employee engagement, satisfaction, and retention
  - Reduced production cost, duration, and error and rework

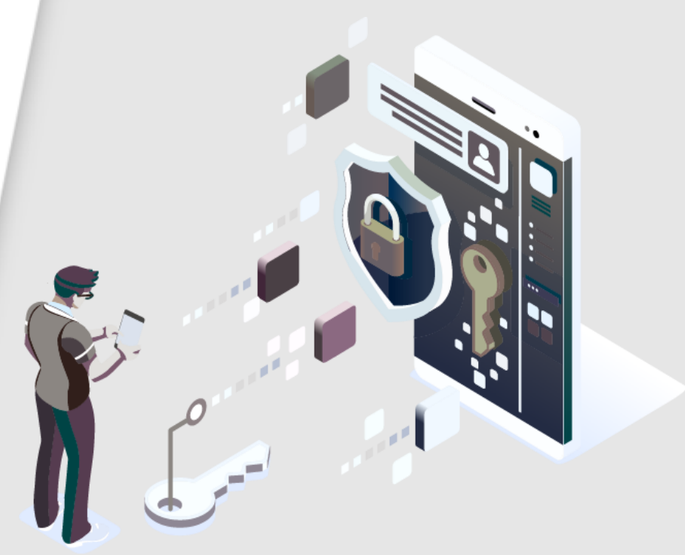
Key Takeaways

- 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.



Key Takeaways

- 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).



This concludes **Security and Risk Management**.

The next domain is **Asset Security.**