ASSIGNMENT 2 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 5: Security		
Submission date	27/03/2023	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Nguyễn Hải Việt	**Student ID**	GCD210136
Class	GCD1101	**Assessor name**	Đặng Quang Hiển

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature	

Grading grid

P5	P6	P7	P8	M3	M4	M5	D2	D3

UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

❒ **Summative Feedback:**		❒ **Resubmission Feedback:**
Grade:	**Assessor Signature:**	**Date:**
Lecturer Signature:		

Contents

Task 1 - Discuss risk assessment procedures (P5)

1. Define a security risk and how to do risk assessment

a) Define a security risk

A security risk assessment discovers, evaluates, and puts into practise the most important security measures in applications. It emphasises avoiding application security flaws and vulnerabilities as well. A risk assessment enables an organisation to examine the application portfolio holistically—from the viewpoint of an attacker. It helps managers make well-informed choices on the use of tools, resource allocation, and security control implementation. The process of risk management for an organisation thus includes completing assessments.

Figure 1: Risk assessment

b) How to do risk assessment

The 4 steps of a successful security risk assessment model:

- **Asset Identification**: List all of your organization's assets, including its physical ones (such as equipment and buildings), its informational ones (such as data and software), and its human ones (such as workers and contractors).
- **Threat Identification**: Look for circumstances or risks that could endanger your assets. This may involve insider threats, social engineering assaults, natural calamities, physical thievery, and more.
- **Vulnerability Assessment**: Analyses areas where your assets are weak or vulnerable so that attackers may exploit them. Old software, flimsy passwords, a lack of access control system, insufficient physical security measures, and other factors may be contributing factors.
- **Impact Estimate**:Determine the probable effects or outcomes of a security breach or event by doing an impact estimate. This might result in business interruption, financial loss, and reputational harm.

2. Define assets, threats and threat identification procedures, and give examples

a) Define assets

Any information that is valuable and may be used to access sensitive information is referred to as an asset. Assets might be data, devices, or other system components inside an organisation.

An employee's desktop computer, laptop, or corporate phone, for instance, would be regarded as an asset together with the software installed on such gadgets. Critical infrastructure is also an asset and includes things like servers and backup systems.

Information assets are the most prevalent assets in an enterprise. These include items like databases and physical files, or the sensitive data you have on hand.

The "information asset container," which is where the information is maintained, is a similar idea. This would be the programme that was used to generate the database in the case of databases. It would be the filing cabinet where the information is kept for physical files.

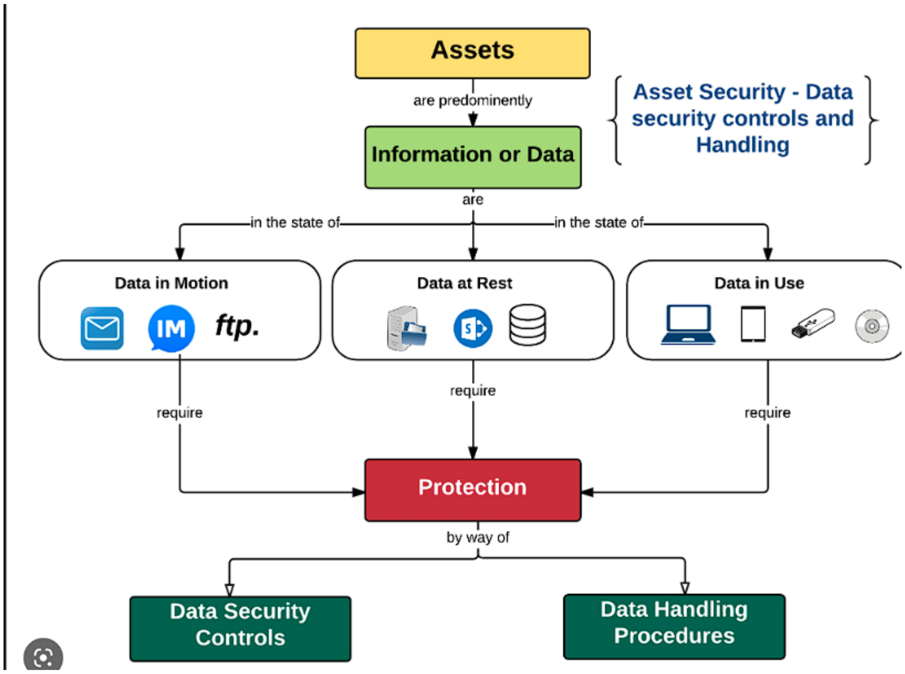


Figure 2: assests

b) Define threats

Any event that may harm an asset, such as if it were stolen, knocked offline, or accessed by an unauthorised person, is considered a danger.

Threats are defined as events that unintentionally or accidentally jeopardise the confidentiality, integrity, or accessibility of an asset.

Accidental threats often entail employee mistake, a technological failure, or an occurrence that results in bodily harm, like a fire or a natural catastrophe, as opposed to intentional threats, which might include things like illegal hacking or a malevolent insider stealing information.

c) Threat identification procedures, and give examples

Procedures for identifying threats: The organisation has to put into place the following procedures in order to detect threats:

Including cybersecurity trends, new threats, active attack groups, and more, research and analyse possible outside and internal dangers to the organisation.

To find patterns or trends in risks, examine previous security events or breaches.

To identify possible risks based on assets, actions, and their effect, conduct security risk assessments.

Example:

- Malware: This is malicious software designed to infiltrate and attack an organization's systems, causing damage such as infection, data encryption, or user activity tracking.
- Data Loss: Includes unauthorized access, use, or disclosure of sensitive organizational information, such as theft of customer information, leakage of employee data, or dissemination of information incorrect information.

- Adverse Weather: Unique weather conditions such as floods, earthquakes, hurricanes, or droughts can jeopardize an organization's physical assets, disrupt business operations, or cause loss of property asset.
- Human error: An employee or member of the organization can make mistakes that err, exaggerate, or fail to follow security rules and procedures, leading to security threats such as data destruction. , disclose information, or steal property.
- Regulatory Violation: Violating an organization's security regulations, laws, or regulations can result in legal threats, loss of reputation, or loss of property.

3. Explain the risk assessment procedure

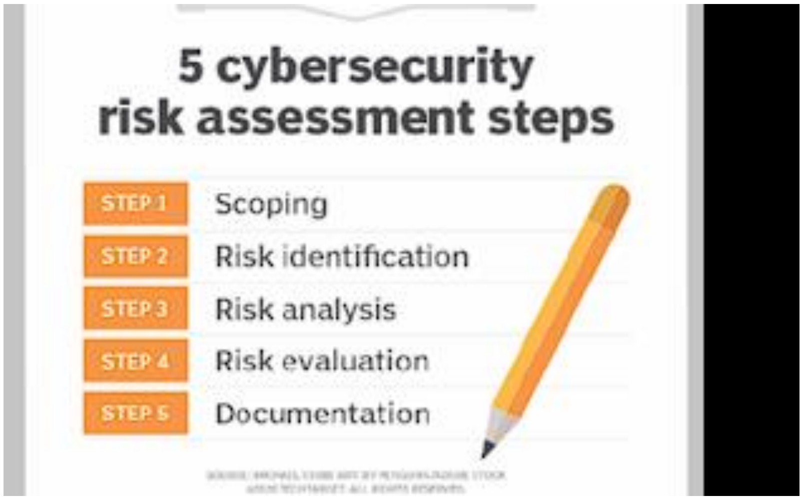


Figure 3: the risk assessment procedure

a) Determine the Scope of the Risk Assessment

Choosing the scope of the risk assessment is the first step. The agreement may cover a whole company, certain departments or locations, or even specific elements like payment processing.

Get all relevant stakeholders on board as soon as the scope is established, especially those whose activities are covered by the evaluation. Their participation is crucial for discovering risks, evaluating repercussions, determining risk tolerance levels, and identifying the relevant processes and assets.

All parties participating in the evaluation process should become familiar with the appropriate terms, such as probability and effect. It promotes risk standardisation and correct communication. For help and clarification on efficient security procedures, organisations could also evaluate frameworks like NIST SP 800-37 and standards like ISO/IEC 27001.

b) Threat and Vulnerability Identification

A threat is any event that can cause damage to an organization's assets or processes. Threats can be internal or external, malicious or accidental.

A vulnerability is a flaw that exposes a company to potential threats. Vulnerabilities can be identified using many methods including automated scanning, auditing, penetration testing, vendor security advisories, and application security testing (AST) techniques.

Your analysis should cover not only technical flaws but also physical and process flaws. For example, a data center that does not have physical access control is vulnerable to physical intrusion, while a server that does not have malware protection is vulnerable to cyber threats.

c) Analyze Risks and Determine Potential Impact

Finding out how the risk scenarios you selected could affect the organisation is the next step. Potential risk (the likelihood that a specific attacker may exploit a vulnerability) is dependent on a number of elements in cybersecurity risk assessment.

- Identification of the security flaw
- simplicity of exploitation
- Threats that may be repeated (some threats are one-time, while others are ongoing)
- prevalence of the danger in the sector or among businesses comparable to it
- Security issues in the past

d) Prioritize Risks

Each risk situation may be categorised using a risk matrix. It is crucial to establish a risk tolerance ratio and outline which danger scenarios go beyond it. You may choose between three possible actions based on the risk matrix:

- Avoid—It could be prudent to take no action if the risk is minor and it is not beneficial to reduce it.
- Transfer—If a risk is large yet impossible to manage, it may be feasible to split the risk by assigning someone else the duty. This may be accomplished by purchasing cyber insurance or hiring an outside security firm.
- Reduce—Risks that are considerable and within the internal team's operating range should be reduced. By implementing security controls and other safeguards, you may lessen their likelihood and possible effects.

Any risk assessment programme must acknowledge that a certain amount of residual risk will be overlooked or underaddressed. Senior stakeholders must explicitly embrace this as a component of an organization's cybersecurity strategy.

e) Document All Risks

It's crucial to record all of the risk scenarios that have been found. To make the current risk portfolio visible, this data should be periodically evaluated and updated.

The risk scenario, date of identification, security measures in place, risk level, risk mitigation strategy, current status, and estimated residual risk after mitigation should all be included in the risk paperwork. There should be a risk owner for each type of risk, who is in charge of managing the danger at a manageable level.

Cybersecurity risk assessment takes time and money since it is a significant and continuing activity. The organisation must iteratively identify and handle new hazards as they arise and as new systems and activities are implemented. A strong first evaluation should serve as a solid foundation for further evaluations.

4. List risk identification steps

a) What is Risk Identification

The process of identifying and evaluating risks to a company, its operations, and its staff is known as risk identification. Risk identification, for instance, could include evaluating possible dangers to the firm, such as accidents, natural catastrophes, and IT security risks like malware and ransomware. Businesses with solid risk management strategies should be able to lessen the effect of risks when and if they do materialise.

b) Risk Identification Process Steps

Risk Identification: Discovering what, where, when, why, and how something can impair a company's capacity to function is the goal of risk identification. A company in central California would include "the possibility of wildfire" as an occurrence that might interfere with normal business operations.

Risk Analysis: In this stage, the likelihood that a risk event will occur as well as the possible consequences of each occurrence are determined. Safety managers might evaluate the amount of rain that has fallen in the previous year and the potential harm that a fire would do to the firm using the California wildfire as an example.

Risk Evaluation: The size of each risk is compared, and each risk is ranked according to its importance and impact. For instance, the impact of a potential wildfire may be compared to the impact of a potential mudslide. Any event that is shown to have a greater chance of occurring and resulting in harm would be ranked higher.

Risk Treatment: Risk response planning is another name for risk treatment. Based on the estimated value of each risk, risk mitigation techniques, preventive treatment, and contingency plans are developed in this stage. Risk managers could decide, using the wildfire example, to keep extra network servers offshore so that operations can continue even if an onsite server is destroyed. Additionally, the risk manager could create arrangements for staff members to evacuate.

Risk Monitoring: Risk management is a continuous process that evolves with time. Repetition and ongoing monitoring of the procedures may ensure that known and unexpected hazards are fully covered.

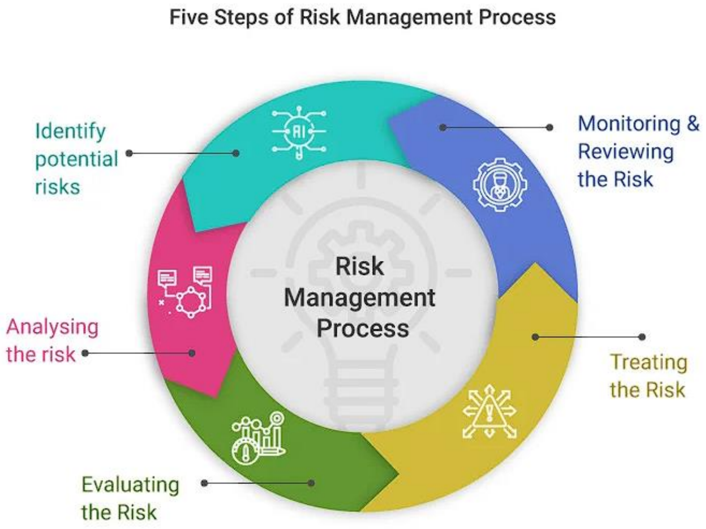


Figure 4: Risk Identification steps

Task 2 - Explain data protection processes and regulations as applicable to an organisation (P6)

1. Define data protection

Data protection is the process of defending sensitive data against loss, tampering, and damage.

Data security is becoming more crucial as data production and storage have expanded at an unparalleled pace. Additionally, since data is used more and more in corporate operations, even a brief period of downtime or a little quantity of data loss may have a significant impact on a company.

Organisations may collapse as a result of the consequences of a data breach or data loss disaster. In light of the fact that the majority of organisations are already bound by some kind of data privacy standard or legislation, failing to secure data may result in monetary losses, loss of reputation and consumer confidence, and legal consequences. One of the main obstacles to digital transformation in organisations of all sizes is data protection.

2. Explain data protection process in an organization

a) Audit of Sensitive Data

You must do an audit of your data before implementing data protection procedures. Determine the storage infrastructure, data types, and sources utilised by the organisation.

Determine what data security mechanisms are currently in place in the organisation, how successful they are, and which may be expanded to safeguard more sensitive data by classifying data into sensitivity categories. Utilising current data security solutions that are "lying around" or are not routinely deployed throughout the organisation is often where the most potential is found.

b) Assessing Internal and External Risks

The organization's security staff should routinely evaluate security threats that might develop both within and outside the organisation. Programmes for data protection must be created with these recognised dangers in mind.

The absence of secure passwords, weak user authentication, inadequate user access control, and unauthorised access to storage services and devices are just a few examples of internal dangers. Insiders who are acting maliciously or accounts that have been hijacked and taken over by threat actors are rising threats.

Social engineering techniques like phishing, the spread of malware, and intrusions into business infrastructure like SQL injection or distributed denial of service (DDoS) are examples of external dangers. Attackers often leverage these and other security risks to access sensitive information without authorization and exfiltrate it.

c) Defining a Data Protection Policy

The organisation should create a data protection strategy that establishes the following criteria based on an examination of its data assets and the most significant threats:

Data protection has a cost, and protection methods must be used in line with the sensitivity of the data. The tolerance for risk for each type of data.

Identify which business apps or user accounts should have access to sensitive data using authorization and authentication policies that take into consideration previous data as well as best practises.

d) Security Strategy

In terms of data protection, a company's security plan should:

- Take action to stop threat actors from gaining access to sensitive data.
- Make sure security measures don't hinder employee access to data when and when they need it or reduce productivity.
- To avoid ransomware or other attacks and to guarantee ongoing data availability, manage backups correctly.

e) Compliance Strategy

Finally, a data protection plan has to take compliance requirements into account. Various laws or compliance requirements that are particular to a given industry may apply to certain organisations or business divisions. The most important laws influencing data protection at the moment are listed below.

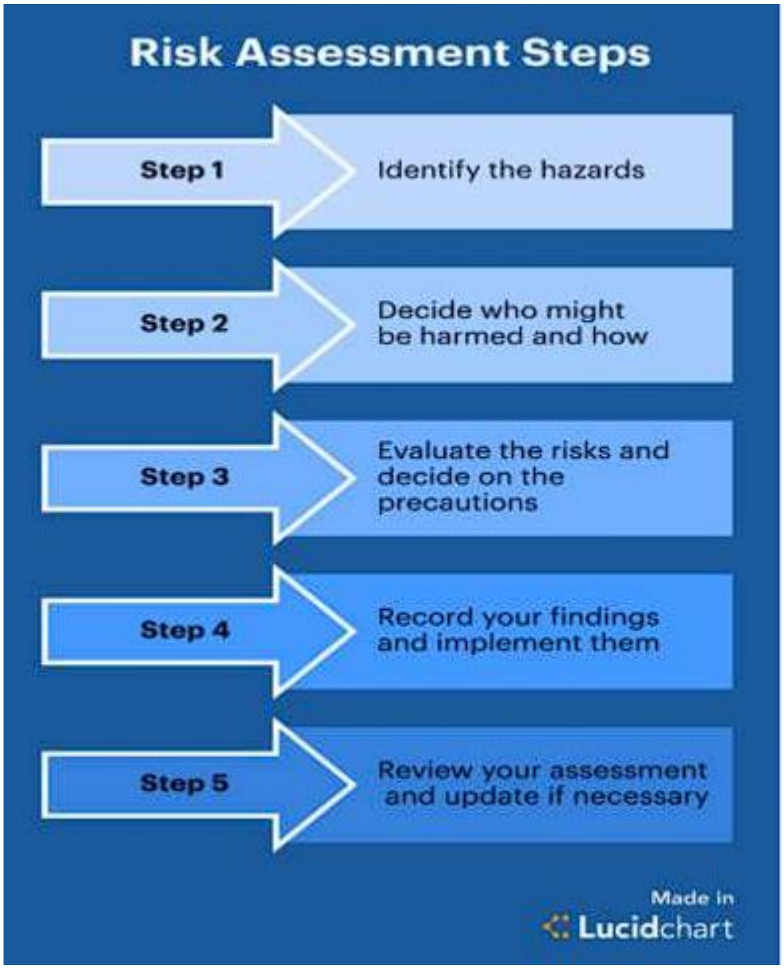

Risk Assessment Steps
Step 1
Identify the hazards
Step 2
Decide who might be harmed and how
Step 3
Evaluate the risks and decide on the precautions
Step 4
Record your findings and implement them
Step 5
Review your assessment and update if necessary
Made in Lucidchart

Figure 5: data protection process

3. Why are data protection and security regulation important?

Privacy protection: Data privacy and confidentiality laws are created to safeguard sensitive and personal information. In order to protect people's privacy rights, they create legal criteria for how organisations acquire, keep, handle, and exchange data. By doing this, it is possible to avoid data abuse, unauthorised access, and breaches that might affect people via identity theft, fraud, or other privacy violations.

Compliance and legal requirements: Laws and regulations at the national, regional, or corporate level often impose data protection and security requirements. In order to protect themselves from legal responsibilities, penalties, fines, and reputational harm, organisations must abide by these rules. Organisations may face serious financial and legal repercussions if they violate data privacy requirements.

Business reputation and trust: Data security and protection priorities show an organization's dedication to protecting the information of partners, employees, and customers. Customers, investors, partners, and regulators are just a few of the stakeholders that benefit from this increased trust and confidence. A solid reputation for data security and protection may provide an organisation a competitive edge, increase client loyalty, and safeguard its brand image.

Data breach prevention: Organisations are often required by data protection and security requirements to establish security controls and procedures to stop data breaches. This comprises steps like monitoring, data backup and recovery, access limits, encryption, and incident response. The danger of data breaches is reduced and sensitive information is shielded from unauthorised access or exposure thanks to these security measures.

Data governance and accountability: Data governance best practises, such as data inventory, data categorization, data retention, and data disposal, are stressed by data protection and security requirements. The integrity, correctness, and dependability of data must be maintained, therefore these procedures encourage accountability, openness, and responsible data management.

Global data transfers: The General Data Protection Regulation (GDPR) of the European Union and other data protection laws have an extraterritorial effect and have an effect on organisations all over the world. In order to guarantee legal and compliant data transfers across borders and reduce risk to their businesses' reputation and bottom line, organisations that handle the personal data of people in several countries must abide by these standards.

Task 2.1 - Summarise the ISO 31000 risk management methodology and its application in IT security (M3)

1. Briefly define ISO 31000 management methodology

The International Organisation for Standardisation (ISO) has released the risk management standard known as ISO 31000. The first edition was published in 2009, and as of this writing, the most current version is from 2018. It provides a set of suggestions meant to assist businesses in streamlining risk management.

Within the larger family of risk management standards known as ISO 31000, ISO 31000:2018 is a single standard. The goal of the risk management standards is to provide the best practise foundation and guidance to all organisations looking to use risk management ideas. They are all designed to be applied broadly across various industries, market segments, and firm types.

The two scopes of risk management are as follows. According to ISO 31000, they are:

- A plan for managing risks. This offers the structural underpinnings and administrative frameworks necessary to plan, administer, monitor, and continuously enhance risk management throughout the whole organisation.
- A procedure for managing risks. This group of management guidelines, guidelines, and practises guarantees efficient risk management. The risk management framework should ideally serve as a guide for the risk management process.

So an organisation to formalise its risk management practises, ISO 31000 provides a set of best practises. With several "silo-centric" risk management systems, this strategy aims to make enterprise risk management more widely adopted by businesses.

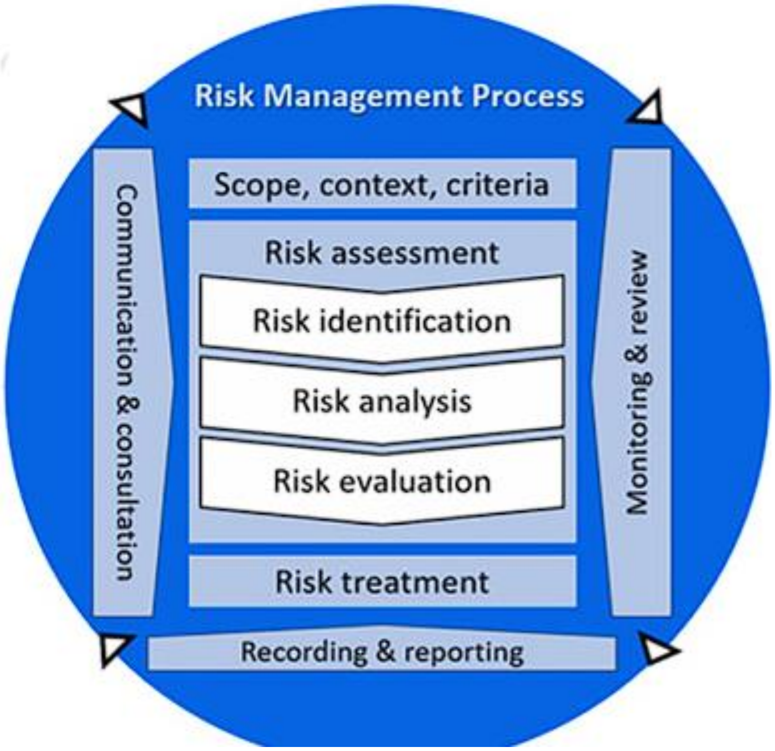


Figure 6: ISO 31000

2. What are its applications in IT security?

Leadership and commitment: A policy stating that enterprise risk management is a goal the organisation wishes to attain would need to be adopted by top executives and the governing body of the organisation (usually the board of directors), after which responsibility for that goal would need to be delegated to particular people.

Integration: Executives should make it clear that risk management must take place throughout the whole organisation and that everyone is responsible for aiding in risk management for the company.

Program design: The programme should be designed to reflect elements like the organization's basic values, business strategy, legal duties, contractual commitments to third parties, and so on. It should also include specific activities that the company will take to manage risk.

Implementation: Create a strategy to put the risk management programme into action, and make sure the plan has enough time and money to carry it out successfully.

Evaluation: Review the risk management programme on a regular basis to examine how effectively it fulfils the objectives that were first set out and to see if any new risks have surfaced that need to be addressed.

Improvement: whether any new actions are required, either to introduce new programme elements to address emerging risks or to enhance programme components that don't meet objectives.

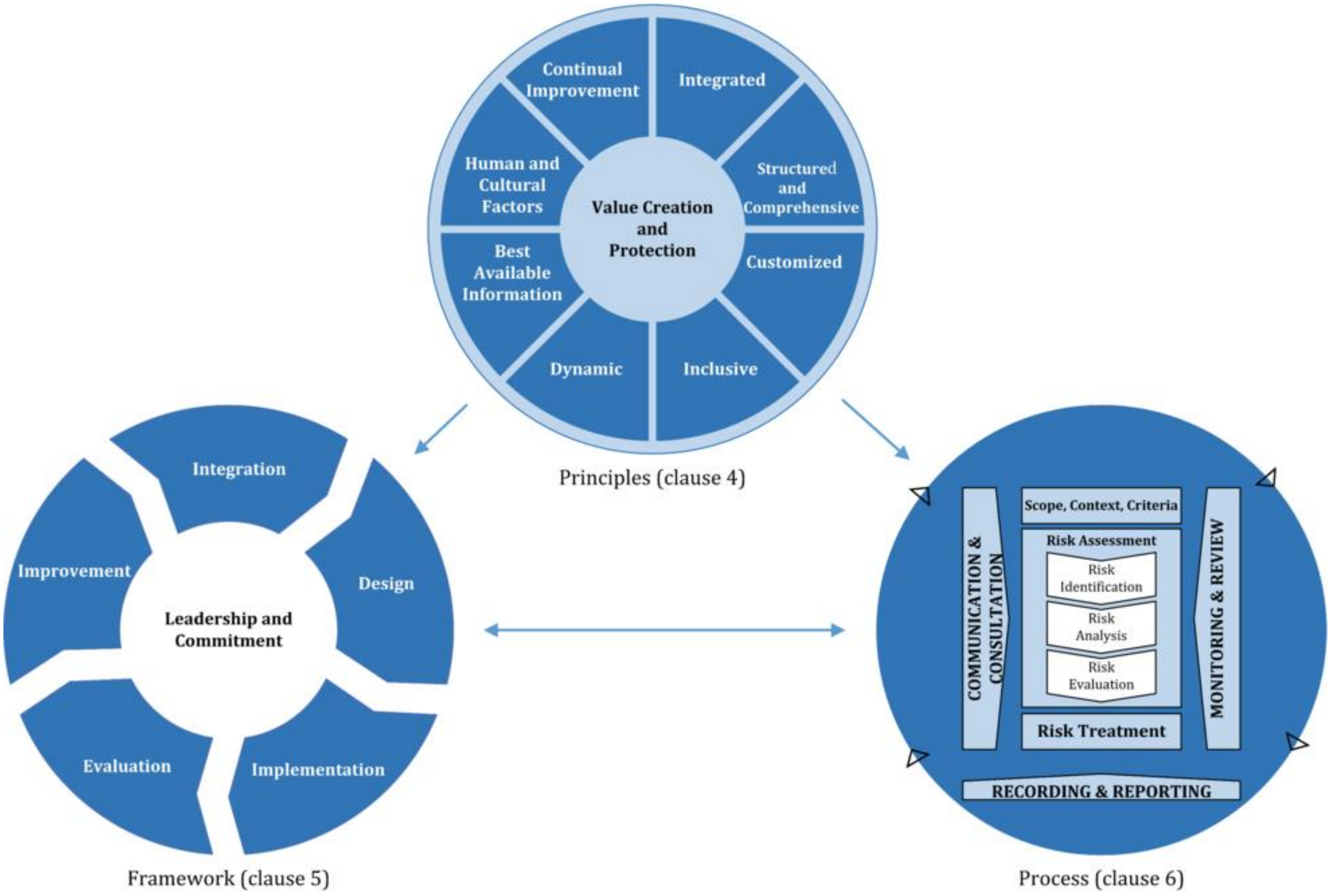


Figure 7: applications in IT

3. Provide a practical example for each of these applications

Leadership and commitment: The senior management and Board of Directors of an information technology company establish a policy that IT risk management is an important goal for the organization. They delegate responsibility for this goal to a Chief Information Security Officer (CISO) who reports directly to the CEO. CISOs are granted the necessary authority and resources to develop and implement an IT risk management program.

Integration: The IT risk management program is integrated throughout the organization, involving all departments and employees. For example, the IT department regularly conducts risk assessments for the company's information systems and networks, while the Human Resources department ensures employees are trained in security awareness and comply with security regulations. Right process. The company's suppliers and partners must also comply with the organization's IT risk management requirements.

Program design: The IT risk management program is designed to align with core values, business strategy, and regulatory obligations. It includes specific steps such as periodically performing IT risk assessments, recommending and implementing IT security measures, monitoring security policy compliance, and ensuring compliance with relevant legal regulations. to IT security.

Implementation: An IT risk management program implementation plan is developed, ensuring that the necessary time and resources are available for effective implementation. The company provides the resources, technology and processes to implement IT security measures, and ensures that staff are trained and knowledgeable about IT security practices and procedures.

Evaluation: The IT risk management program is periodically evaluated to assess the extent to which initial objectives have been achieved and to identify new threats that may emerge that require attention. The Company conducts an evaluation of the effectiveness of its IT risk management program, based on performance indicators, security test results, reassessment of potential threats, and feedback from users and threats Stakeholders.

Improvement: The company takes necessary steps to improve parts of its IT risk management program that fall short of expectations or implement new elements of the program to deal with emerging threats. For example, based on the assessment, the company can adjust policies, procedures, or invest in new technology to improve IT risk management.

Task 2.2 - Discuss possible impacts to organisational security resulting from an IT security audit (M4)

1. Define IT security audit

A security audit evaluates a company's information system's security systematically by gauging how closely it adheres to predetermined standards. A comprehensive audit often evaluates the security of the system's software, information handling procedures, user behaviour, and physical setup and surroundings.

Security audits are often used to ascertain compliance with laws that stipulate how businesses must handle information, such as the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, and the California Security Breach Information Act.

Along with vulnerability analyses and penetration testing, these audits are one of the three primary categories of security diagnostics. Security audits compare the effectiveness of an information system to a set of standards. An extensive examination of an information system to identify possible security flaws is known as a vulnerability assessment. A security specialist will use a covert technique called penetration testing to check a system's resistance to a particular assault. Each strategy has its own advantages, and the most successful strategy may include combining two or more of them.

2. What possible impacts to organisational security resulting from an IT security audit

- Detect system vulnerabilities, security issues and weaknesses, increasing the likelihood of being attacked or compromised.
- Define a security benchmark to compare with future security audits to help gauge an organization's progress in protecting information and systems.
- Ensure that the organization adheres to internal security policies, put in place protections and mitigate risks.
- Comply with security regulatory requirements from external organizations, such as government agencies, customers, or business partners.
- Evaluate the effectiveness of security training and identify ways to improve security awareness and awareness within the organization.
- Detect and remove unnecessary resources to reduce risk and ensure the safety of information and systems.

3. Provide a practical example for each of these impacts

Identify security issues and gaps: When a company performs an information security audit, it may discover that it is using outdated or vulnerable devices, resulting in security risks.

Set security standards: Information security audits can help define a basic security standard for an enterprise, helping to compare and evaluate the effectiveness of security measures later.

Comply with the organization's internal security policies: Information security audits help ensure that the organization adheres to security policies that are established to reduce security risks.

Compliance with external security regulatory requirements: Information security audits can help ensure that an organization is in compliance with security regulatory requirements from other government organizations or security regulations.

Determine if security training is sufficient: Information security audits help assess the level of security training employees have in the organization and help determine if it is sufficient to reduce security risks.

Identify unnecessary resources: Information security audits help an organization identify resources that are no longer needed, such as applications that are no longer in use, helping to reduce the security risks associated with keeping these unnecessary resources.

Task 3 - Design and implement a security policy for an organisation (P7)

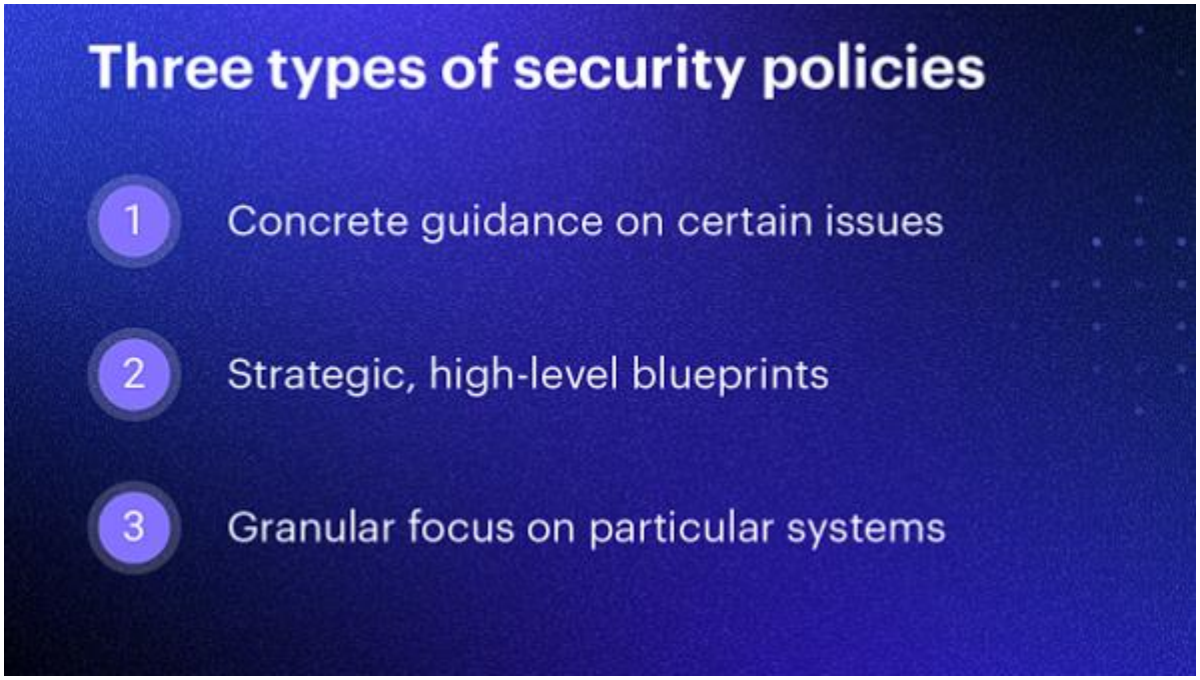
1. Define a security policy and discuss about it

a) What is a security policy?

A security policy, also known as an information security policy or an IT security policy, is a written statement of the guidelines, standards, and general strategy that a company employs to protect the privacy, integrity, and accessibility of its data. There are many distinct types of security policies, ranging from high-level frameworks that outline an enterprise's overall security objectives and guiding principles to papers addressing more specialised concerns like remote access or Wi-Fi usage.

Standard operating procedures and other forms of documentation, such as a security policy, are typically used together. Together, these papers aid the business in achieving its security objectives. The other papers assist provide structure around the practise, with the policy defining the overarching strategy and security position. A security policy may be thought of as providing the "what" and "why," while guidelines, standards, and procedures provide the "how."

b) Three types of security policies



Three types of security policies

1 Concrete guidance on certain issues

2 Strategic, high-level blueprints

3 Granular focus on particular systems

Figure 8: type of security policies

a) Program policy

Information security programme policies are strategic, high-level blueprints that direct an organisation. They outline roles and duties, compliance methods, and the program's aim and scope in detail. These papers, often known as master or organisational policies, are usually technology-neutral and are created with significant participation from top management. They should be drafted at a high enough level to be applicable even after organisational and technological changes, therefore they are the sort of policy that is least regularly revised.

b) Issue-specific policy

Issue-specific policies expand on the general security policy and provide more particular direction on certain matters that concern the workforce of an organisation. Examples of typical policies include those governing network security, BYOD (bring your own device), social media, and remote work. These may cover certain technological fields, although they are often more general. A company-approved and supported VPN may be the sole means of obtaining offsite access, according to a remote access policy, although the policy is unlikely to mention a particular VPN client. The business may switch suppliers in this manner without undergoing significant changes.

c) System-specific policy

The most specialised kind of IT security policy, a system-specific policy focuses on a certain kind of system, such a firewall or web server, or even a single computer. System-specific policies, as opposed to issue-specific rules, may be more relevant to the technical staff that maintains them. According to NIST, system-specific policies should include both an operational set of rules and a security purpose. Although senior management continues to make the most important choices and regulations, IT and security teams have a significant role in the development, implementation, and enforcement of system-specific policies.

2. Give an example for each of the policies

a) Guides the implementation of technical controls

A security policy outlines the intents and expectations of senior management with respect to security, but it does not provide precise low-level technical assistance. The security or IT teams are then responsible for translating these ideas into precise technological actions.

A policy could specify, for instance, that only authorised users should be permitted access to confidential corporate data. This policy's particular authentication procedures and access control guidelines may alter over time, but its overall goal never changes. The security or IT teams are forced to make educated guesses as to what top management wants without a starting point. As a result, security rules may not be applied consistently by various organisations and commercial enterprises.

b) Sets clear expectations

Without a security policy, it will be up to each employee or user to exercise their own discretion to determine what is and is not acceptable. When various personnel use different standards, this may be disastrous.

Is using a work gadget for personal use acceptable? Can a management, out of convenience, share passwords with their direct reports? How about using unauthorised software? Without defined rules, various workers could provide different answers to these queries. Additionally, a security policy should specify how compliance will be checked for and enforced.

c) Helps meet regulatory and compliance requirements

Assist in fulfilling legal and compliance requirements: Laws like HIPAA and Sarbanes-Oxley, as well as rules and standards like PCI-DSS, ISO 27001, and SOC2, demand that privacy policies be in writing. A security policy is often necessary in developing a plan to fulfil the ever-increasing demands for data privacy and security, even when it is not officially mandated.

For instance, to be HIPAA compliant, a business in the healthcare sector must have a written privacy policy that directs the safeguarding of sensitive patient medical information. Specific controls, methods, and procedures should be included in this policy in order to meet HIPAA regulations.

d) Improves organizational efficiency and helps meet business objectives

Supports the development of a security culture: A security policy may be crucial in fostering a security culture inside an organisation. It offers precise instructions, expectations, and a framework for gauging and monitoring compliance.

For instance, a privacy policy can specify that each employee must undergo yearly security training and promptly disclose any security breaches. This lowers security risks, motivates workers to actively engage in the protection of information, and helps establish a culture of security awareness inside the organisation.

3. Give the most and should that must exist while creating a policy

Purpose: Clearly define the purpose of the security policy, including protecting the organization's information, resources, systems, and operations from threats and risks.

Scope: Clearly define the scope of the security policy, including the systems, data, applications, devices, and other resources to which the policy applies.

Principles and regulations: List in detail the security principles or provisions that the policy defines, including authentication procedures, access control, data encryption, and security incident reporting.

Directory management: Clearly define roles, responsibilities, and permissions for users, and manage categories of access rights and permissions based on "need to know" and "need to" principles.

Monitoring system: Define a mechanism to monitor, track, and test the effectiveness of the security policy, including monitoring user activities, detecting and dealing with security incidents, and monitoring monitor security systems.

Security Incident Handling: Put in place security incident handling procedures, including reporting, investigating, evaluating, and dealing with security incidents in a timely and effective manner.

Security awareness and training: Specify security awareness and training requirements for employees and users, including helping them recognize and respond to security threats.

Test and review: Define procedures for testing, evaluating, and re-evaluating the security policy, including policy compliance testing.

Compliance with laws and regulations: Ensure that the privacy policy fully complies with the laws, regulations, and standards related to information security, including those relating to the protection of personal data, GDPR, HIPAA, PCI DSS compliance, etc.

Incident prevention and response: Put in place security incident prevention and response measures, including implementing safeguards, backing up data regularly, and having an incident response plan to minimize the impact of security incidents.

4. Explain and write down elements of a security policy

a) Clear purpose and objectives

When it comes to programme policies, this is extremely crucial. Keep in mind that many workers are unaware of security dangers and may consider any security measure to be a burden. The whole of the organisation should be made aware of the significance of information security by a clear mission statement or purpose stated at the highest level of a security policy.

b) Scope and applicability

No matter what kind of security policy it is, it should always include a scope or declaration of application that specifies to whom the policy applies. As long as it is clearly defined, this might be based on a particular geographical area, business unit, job type, or other organisational notion.

c) Commitment from senior management

Security guidelines are intended to convey senior management's intentions, preferably at the C-suite or board level. Any security programme is likely to fail without support from this level of leadership. Your rules must be explained to staff, updated often, and consistently applied if you want them to be successful. All of this becomes challenging, if not impossible, in the absence of managerial support.

d) Realistic and enforceable policies

You must keep in mind that your workers live in the real world even if it may be tempting to build your security strategy on a flawless example. A policy that is unduly onerous is unlikely to be broadly accepted. A policy without a way to enforce it might also be readily disregarded by a sizable portion of personnel.

e) Clear definitions of important terms

Keep in mind that a security policy's target audience is often non-technical. It's crucial to use straightforward, jargon-free language, and any technical words used in the text should be clarified.

f) Tailored to the organization’s risk appetite

Although risk cannot ever be totally eradicated, management of any organisation must determine the acceptable amount of risk. This risk tolerance must be considered when developing a security policy since it will influence the subjects that are covered.

g) Up-to-date information

Updates to security policies are essential for keeping them effective. The programme or master policy should nevertheless be examined on a regular basis even if it may not need frequent changes. As technology, labour patterns, and other variables evolve, issue-specific rules will need to be modified more often. Over time, you could discover that more new policies are required: BYOD and remote access rules are two excellent instances of regulations that have just recently become commonplace.

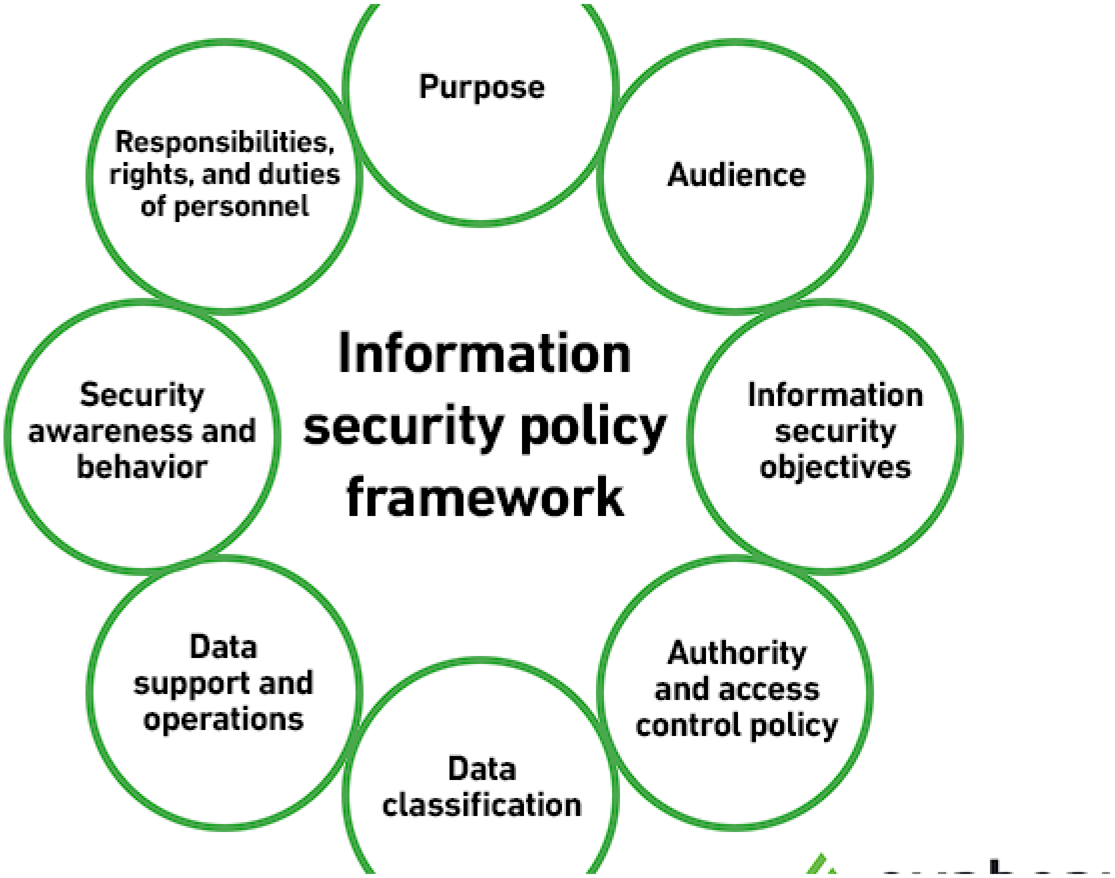

Purpose
Audience
Information security objectives
Authority and access control policy
Data classification
Data support and operations
Security awareness and behavior
Responsibilities, rights, and duties of personnel
Information security policy framework

Figure 9: elements of a security policy

5. Give the steps to design a policy

a) Step 1: Identify the Need for a Policy

Creating procedures for every unanticipated circumstance limits management's capacity to handle employee demands and unique situations. Clear policies guarantee fair and lawful practises. Employers may create a policy:

- If workers' behaviour reveals uncertainty about how to act (e.g., attendance policy, mobile usage policy, travel cost policy, code of conduct).
- If the organisation needs legal protection (e.g., investigations policy).
- If federal rules and regulations must be followed (e.g., COBRA, FMLA).
- Progressive discipline requires constant norms and regulations.
- If workers require consistency and fairness (e.g., paid time off, benefits eligibility).

b) Step 2: Determine Policy Content

Policies outline company expectations and employee treatment. New policy should avoid restrictive wording that must be obeyed precisely as stated. The phrasing should be flexible and avoid contractual guarantees. Organisations shouldn't:

- Say the organisation "only" or "always" does something or "will" or "must" behave a certain manner.
- Call workers "permanent."
- Only fire "for cause."
- Guarantee employment.
- Use all-inclusive lists in disciplinary and work rules.

Employers should utilise "generally," "typically," "usually," and "may" so managers may interpret and enforce rules depending on the circumstances and severity of any company policy violation(s).

Policies must be written clearly. Employers' policy wording varies by size, industry, and occasionally geography. Most policies share elements. Below are typical components:

- **The objective:** The purpose statement explains why the organisation is issuing the policy and its expected consequence. "Employees contribute to [Company Name]'s corporate culture and reputation in how they present themselves," for instance. To impress consumers, regulators, and firm shareholders, dress professionally. Good grooming and proper clothes generate staff pride and confidence."
- **The specs**: This section describes the policy's rules, requirements, and organisational behaviour standards. "Employees must wear business attire Monday through Thursday," for instance. Unless there is a workplace event or a meeting with external customers or suppliers, Fridays are casual dress days.
- **Implementation part**: This section lists who is accountable for policy declarations and how they will enforce them. "Managers will exercise discretion in determining appropriateness in appearance."
- **Effective date**: As of The policy begins on this day. Example: "All employees will be subject to this new policy/revision as of [date]."
- **Glossary**: Definitions of policy terminology (e.g., "casual shirts: All shirts with collars, including collared blouses, golf and polo shirts.").

Employers may write rules to meet business requirements, but they must follow employment regulations. Multistate firms must ensure that rules do not contradict with several state employment regulations, making this more difficult. Before presenting rules to workers, professional legal counsel should evaluate them.

c) Step 3: Obtain Stakeholder Support

Too frequently, people required to execute and enforce rules are not contacted before implementation. After the policy is written, managers and supervisors must be communicated with (e.g., meetings, emails, teleconferences) to implement it. This communication should explain why the new policy (or amendment) is required, how it will affect the stakeholder's area(s), and any stakeholder concerns. These discussions will determine policy adjustments before legal counsel reviews them.

d) Step 4: Communicate with Employees

When feasible, companies should explain why the policy is being imposed. Employees should be provided enough information to understand the company's stance without complicating conversations. Based on the policy's nature, sensitivity, and simplicity of understanding, employers may decide how to convey it. The optimum way to distribute the policy—email, memo, or individual/small group/all-employee business meetings—must also be chosen. Email and corporate memos should stand out from other normal messages that workers may neglect. Organisations may alter the subject header, email significance, backdrop and font, memo distribution mode, and email read receipts.

Employees should have a way to raise policy questions. The policy should include an acknowledgement statement that the employee received and understood the new policy and its effective date. Employees should sign and date the policy. It should be incorporated to the employee handbook, intranet, and new-hire orientation programmes. Employers should tell workers how to obtain the policy later (intranet connections, policy attachment to print and put to employee handbook).

e) Step 5: Update and Revise the Policy

Well-written, frequently reviewed rules may improve employee relations and communication. They demonstrate the company's workplace positivity. Written rules may be used to prove nondiscrimination and defend against employee claims.

To comply with federal and state legislation and organisational demands, policies should be evaluated often. New laws, regulations, and court judgements may change policy wording and employer implementation. Most experts advise annual policy reviews. In the meantime, employers should subscribe to a service or magazine or join an HR or employment organisation. Government Affairs updates SHRM members on state and federal laws and future or proposed legislation that may affect HR professionals.

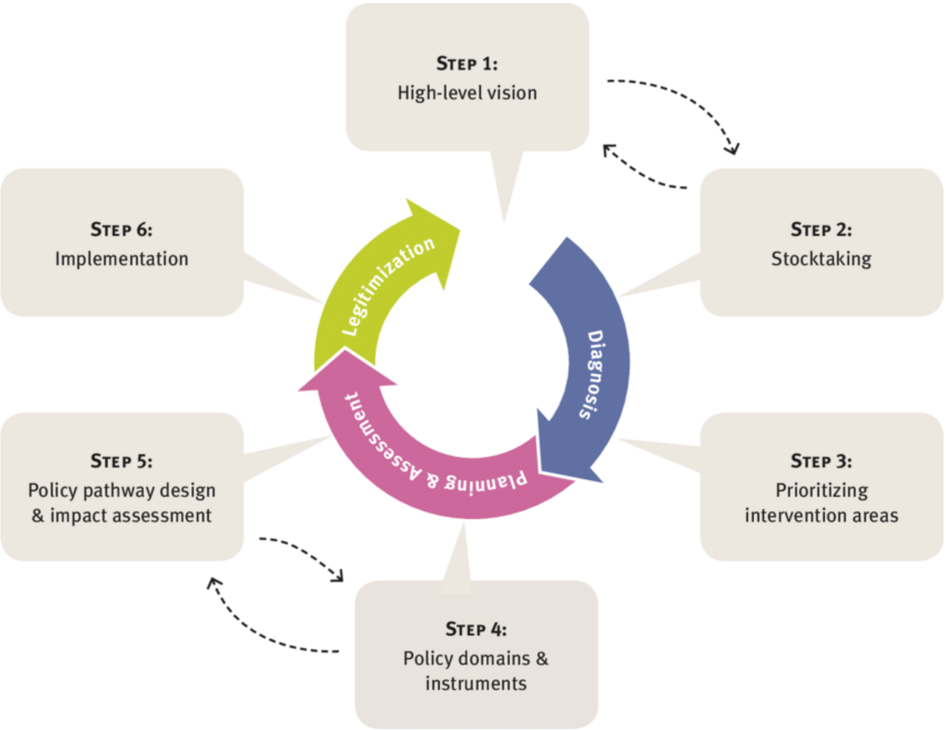


Figure 10:steps

Task 4 - List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion (P8)

1. Discuss with explanation about business continuity

a) Define

Business continuity is the capacity of an organisation to continue essential business and service activities in the face of a variety of crises, including natural disasters, technical setbacks, employee mistakes, or other unanticipated circumstances. Developing strategies, rules, and processes as part of business continuity planning (BCP) enables an organisation to retain its essential operations and bounce back swiftly. very little effect on operations, reputation, and stakeholders following an event.

Figure 11: business continuity

b) Why business continuity is important

Because business continuity can make or break a company, top companies prioritise it. Critical business functions must be restored quickly. Business continuity plans may save time and money. The recovery plan must contain roles, responsibilities, and system recovery sequence. Business continuity has numerous components to consider and test, so plan ahead. For huge data sets, failover to a faraway data centre may be a better option than restoring from a backup.

A contingency plan is a final choice when resilience and recovery plans fail or an unexpected incident happens. Last-resort contingency plans are practised. These demands might include hiring third-party contractors or locating a second site for emergency office space or remote back-up servers.

c) Business continuity and disaster recovery

Disaster recovery and business continuity are intertwined. Businesses may save tens of thousands of dollars and even decide whether to survive the effects of a natural catastrophe by having a business continuity and crisis management strategy in place. Businesses have a far higher chance of returning to normal sooner after a catastrophe if they have a sound business continuity plan and well-managed disaster recovery tools. In a perfect world, well-prepared companies would be able to go on with business as usual. Businesses that lack a business continuity plan and disaster recovery strategy are significantly more susceptible to being destroyed by a natural catastrophe or cyberattack.

2. List the components of recovery plan

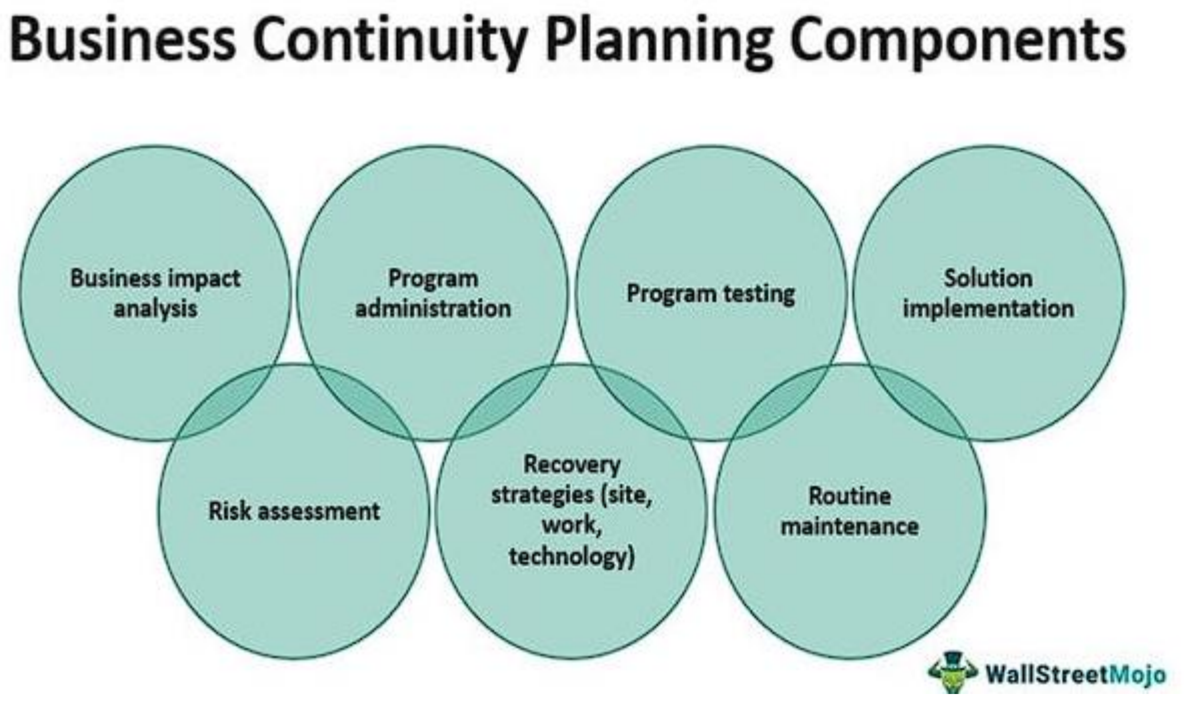


Figure 12: the components of recovery plan

a) Complete Inventory of Hardware/Software/Other Equipment

You must consider what resources would need to be retrieved while drafting a disaster recovery strategy. Every piece of hardware, software, and peripheral that interacts with your networks or is utilised by your staff, subcontractors, and suppliers must be thoroughly inventoried.

You will need to take into consideration every on-premise, cloud-based, mobile/BYOD product and technology your organisation utilises, so this will be a really big undertaking.

b) Documented Business Objectives

DR often involves business considerations more so than IT ones. So that you know where to concentrate first during recovery, it is crucial to include all business units and stakeholders in the discussion about company goals.

To make sure all systems are taken into consideration, start by mapping out the complete architecture. Setting priorities can help you guarantee that the most crucial systems and applications are operational first once you are aware of what you are safeguarding.

To aid with recovery attempts, divide systems and applications into three tiers:

- Critical to the mission: These take precedence. In order to prevent significant data loss and serious business operations interruption, get these systems back online right away.

- Essential: The firm won't suffer significantly if these less important systems are down for up to 24 hours.
- Applications are the least important since the company can function without them for a few days.

c) Defined Tolerance for Downtime and Data Loss

You may set recovery time goals (RTO) and recovery point objectives (RPO) after you have your defined business objectives in hand. You will use these metrics to estimate how much downtime and data loss you can tolerate. In other words, these metrics let you to assess how long an application can be down for without significantly harming the company (RTO) and how much data may be lost before this happens (RPO).

d) A DR Team

During a crisis, a skilled DR team is crucial. Since each team member has been given a distinct role, it is clear who is in charge of what aspect of the recovery effort.

This team will serve as a point of contact for stakeholders and be in charge of communications during the crisis. The responsibility for training workers in emergency response rules and procedures is placed on the disaster response team.

e) Alternative Workspaces

Your business space could not be usable in the case of a fire or other tragedy. It will be easier to keep the firm running as normally as possible if there is a strategy in place to allow staff to work remotely.

Ensure that every employee has access to a laptop and an internet connection, or can easily get one. And maintain accessibility by setting up backup email and phone system options that provide crucial lines of contact for workers, clients, and suppliers.

f) Remote Access

Accessing business data and apps remotely may be a security issue, regardless of whether you're using VPN, RDP, SSH, or another access-control solution. When COVID-19 issues suddenly required millions of people to work from home, this became extremely clear.

It's not a good idea to discover that your infrastructure isn't capable of securely handling remote access in the midst of a crisis. To guarantee that your data can be securely accessible from outside the firewall, update your security technology right away.

g) Secure Backups

Your DR attempts will succeed or fail depending on the consistency and quality of your backups. Consider the following recommendations for keeping backups safe and accessible in case you need them in an emergency:

- Maintain a backup system that is isolated from and unreachable from the primary corporate network. Some ransomware has the ability to traverse the network, encrypt backup data, and make it worthless.
- Use a 3-2-1 backup method by making three copies of your data, putting them on two different types of media, and putting one of them off-site or in the cloud.
- Invest in a cloud backup and DR solution that streamlines backup and recovery by offering a central UI and the most up-to-date tools and technologies for disaster recovery.

h) A Comprehensive Testing Strategy

Don't wait for a real crisis to see how well your DR strategy functions. Immediately put in place a thorough testing plan (and implement it). Three goals should be reached by your strategy:

- To ensure that your data is secure and retrievable, test your backups.
- Make sure your DR procedures are tested.
- Test your staff to ensure they are aware of what to do in an actual emergency.

3. Write down all the steps required in disaster recovery process

a) Know Your Threats

Map out the hazards you are most likely to encounter by learning about the past of your company, the industry, and the area. Natural catastrophes, geopolitical occurrences like wars or civil unrest, malfunctions of vital technology like servers, Internet connections, or software, and cyberattacks that are most likely to have an impact on your line of work should all be included.

Make sure your disaster recovery strategy is effective against all risks, or at the very least the most probable or serious ones. Create distinct DR plans or parts within your DR plan, if appropriate, for various sorts of catastrophes.

b) Know Your Assets

It's critical to be thorough. Make a comprehensive inventory of all the assets that are necessary for your company's ongoing operations with the help of your staff. This covers network hardware, servers, workstations, software, cloud services, mobile devices, and more in the context of IT. After making your list, group it into:

- Your firm cannot function without essential resources, such as an email server.
- Important resources that may substantially impede certain operations, like a presentation projector
- Other assets that won't significantly affect the firm, such a recreational system utilised by staff members during lunch

c) Define Your RTO and RPO

For important assets, provide your Recovery Time Objective (RTO). How much idle time can you stand? For instance, every minute of outage causes significant financial harm to an eCommerce site with considerable traffic. If there is no data loss, an accounting business may be able to withstand a day or two of downtime before things go back to normal. Create a procedure and get the tools necessary to use the RTO's operations once again.

Recovery point objective (RPO) is the maximum age of data that an organisation must recover from backup storage in order to go on with business as usual after a catastrophe. RPO is used by organisations to establish the minimal backup frequency. A four-hour RPO, for instance, necessitates backing up at least once every four hours.

d) Set Up Disaster Recovery Sites

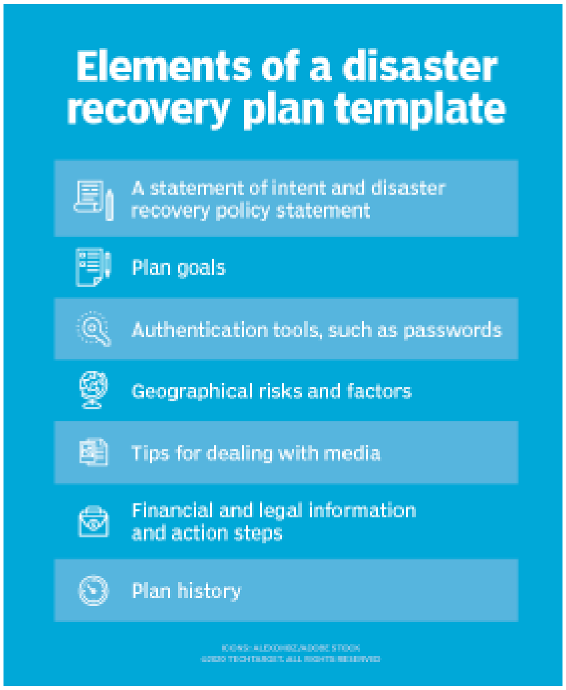
Having a mechanism to duplicate data across several disaster recovery locations is a key component of practically any disaster recovery strategy. Although many firms plan regular data backups, the best strategy for disaster recovery is to continually duplicate data to another server.

Local storage has a shorter RTO but is less catastrophe resistant. Additionally, it enables more regular data replication and backup, which enhances your ability to recover data from almost any point in time (RPO).

e) Test Backups and Restoration of Services

Backups may fail in a crisis just like business systems do. There are several horror tales of businesses who installed backup systems but found out too late that the backups weren't truly operating. You may not be aware of a setup issue, software bug, or equipment failure that renders your backups unusable until you test them.

Testing that data is being copied accurately to the destination site is an essential component of any disaster recovery strategy. Testing if it is feasible to restore data to your production site is equally crucial. When you set up your disaster recovery system, you must do these tests. Then, you must repeat them on a regular basis to make sure the arrangement is still functional.



Elements of a disaster recovery plan template

A statement of intent and disaster recovery policy statement

Plan goals

Authentication tools, such as passwords

Geographical risks and factors

Tips for dealing with media

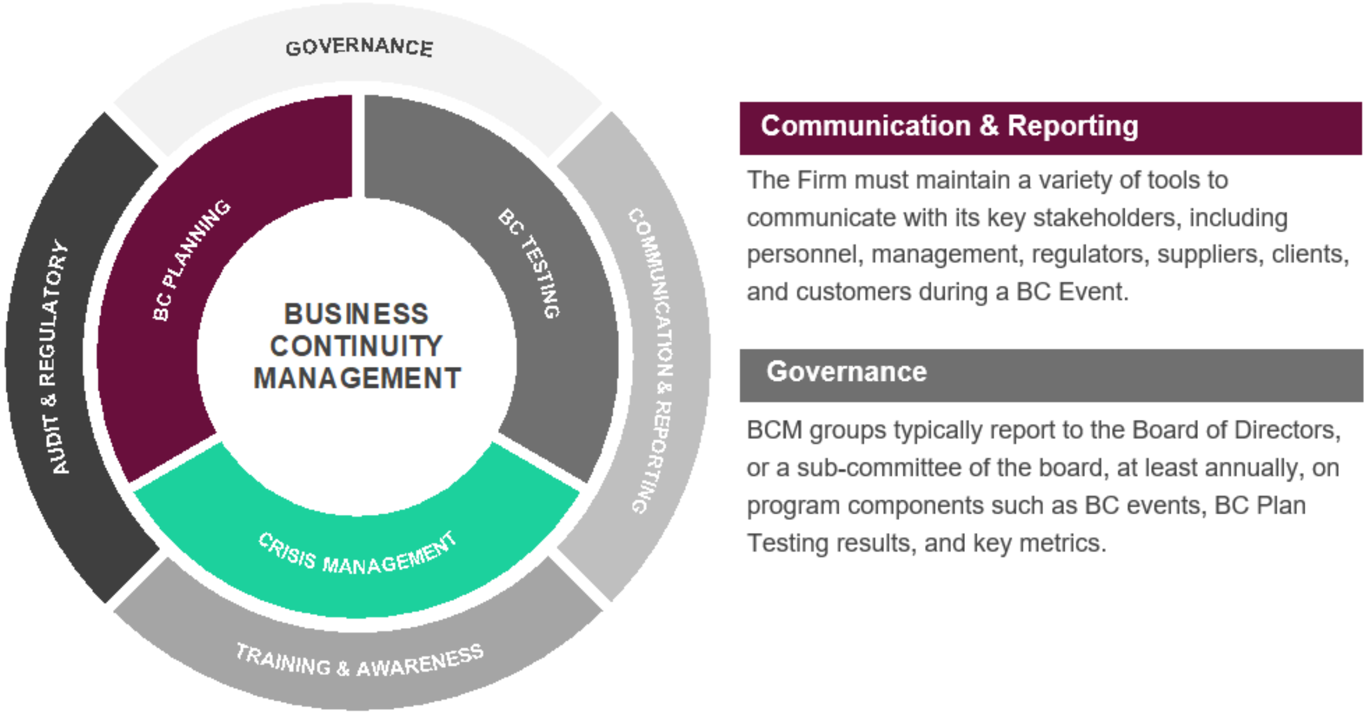
Financial and legal information and action steps

Plan history

ICONS: ALEXDNDZ/ADOBE STOCK
©2020 TECHTARGET. ALL RIGHTS RESERVED

Figure 13: disaster recovery process

4. Explain some of the policies and procedures that are required for business continuity



Communication & Reporting

The Firm must maintain a variety of tools to communicate with its key stakeholders, including personnel, management, regulators, suppliers, clients, and customers during a BC Event.

Governance

BCM groups typically report to the Board of Directors, or a sub-committee of the board, at least annually, on program components such as BC events, BC Plan Testing results, and key metrics.

Figure 14: some of the policies and procedures

Business Impact Analysis (BIA): A thorough evaluation of the resources, procedures, and operations vital to the organization's operations is included in this policy. It is beneficial to assess the probable effects of occurrences on these crucial areas and to rank them according to the organization's importance.

Risk Management Policy: This policy outlines the methods and guidelines for locating, evaluating, and controlling risks that might have an adverse effect on the organization's operations. In order to lessen the effect of risk on business continuity, it involves risk assessment, risk mitigation, and risk monitoring.

Incident Response Plan (IRP): This plan outlines the processes and accountability for handling situations when events or interruptions may have an impact on the organization's operations. It outlines how to identify and report events, mobilise reaction teams, and plan for communication and recovery efforts.

Data Backup and Recovery Policy: This policy specifies the frequency and security of data backups as well as the steps to be taken in the case of data loss or system failure. It involves off-site data storage, monitoring the use of data recovery processes, and protecting backup data from unauthorised access.

Emergency Communication Plan: The processes and guidelines for communication during emergencies or disruptions are outlined in this plan. To maintain consistent and timely communication with stakeholders within and outside the organisation, it also involves designating spokespersons, communication channels, and message templates.

Task 4.1 - Discuss the roles of stakeholders in the organisation to implement security audit recommendations (M5)

1. Define stakeholders

In simple terms, Stakeholder means stakeholders, which can be an individual, a group of people, or an organization that have an interest in the operation and success of a project.

Stakeholders can include the following groups of people: suppliers, members, internal employees, customers, external investors or regulators.

Determining the right Stakeholder is one of the factors that determine the success of the project. If the Stakeholder is not sure, your project is unlikely to succeed. So, right from the start, be smart when choosing Stakeholders to join your project.

Figure 15: stackholder

2. What are their roles in an organization?

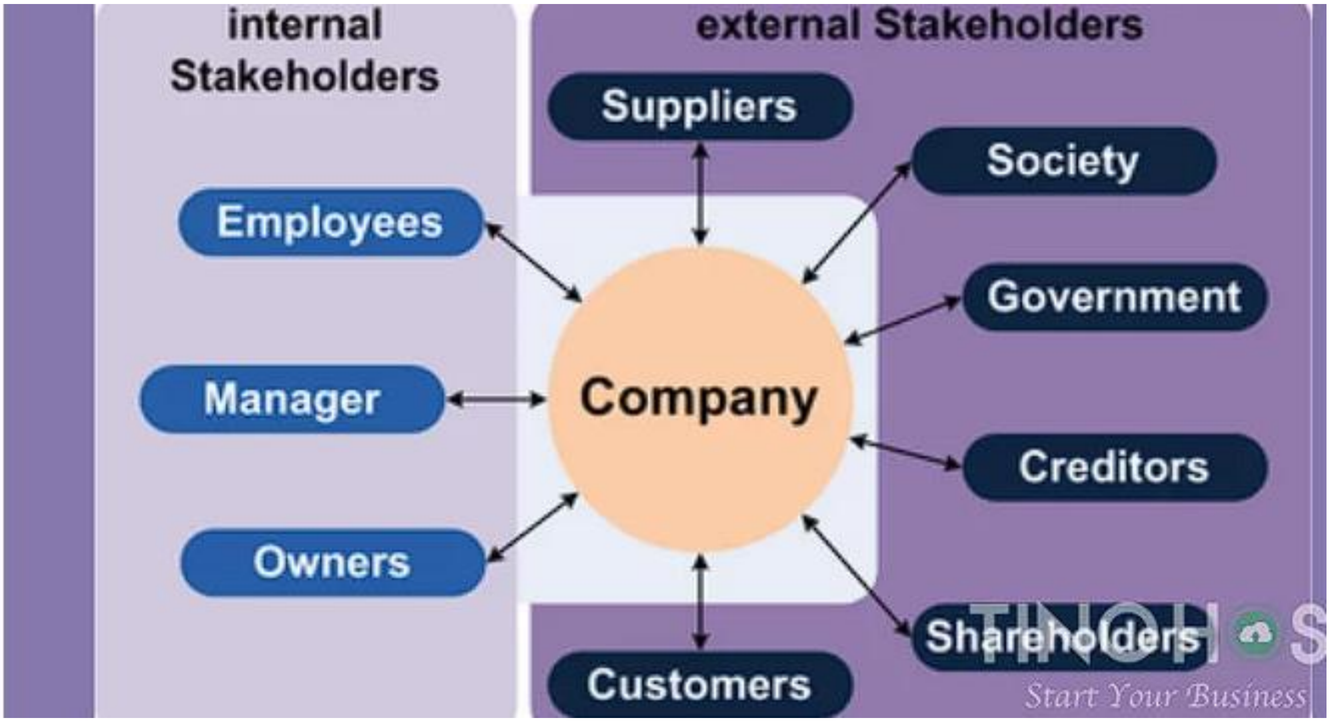


Figure 16: role is an organization

a) Client

This stakeholder's concern is the quality of the company's products, services, or core values. Businesses want to survive because of the consumption of customers. Therefore, no one can deny the role and contribution of this stakeholder in the development of the company because it is they who perceive and consume the product.

b) Staff

Salary, working environment and advancement opportunities are the concerns of this stakeholder. They are a key component of the business, in charge of the entire operation and production process to get the finished product to the consumer. Therefore, their contributions will directly affect the company internally.

c) Investors, sponsors

They care mainly about capital, financial as well as profit issues. Not every company has this stakeholder. However, if your business has stakeholders who are investors and sponsors, you won't need to worry about money problems when you now have stakeholders to support your business.

d) Supplier

For suppliers, revenue is what they care about after providing and supporting businesses. Depending on the business situation, suppliers will influence the market price to ensure they get a profit after making an agreement with the company. Therefore, this stakeholder also contributes significantly to the working and development mechanism of the organization.

e) Community

This is a common form of stakeholder mainly in large enterprise models. They will be an invisible factor affecting economic development. Moreover, the influence of a large business entity also contributes to changes in income, quality of life, security, environment, etc. of a certain community group or area.

f) Government

This external stakeholder's interest is focused on tax, GDP, and social security issues. Although it does not have a strong influence on the company, the adjustment of policy or statutory provisions will unintentionally affect the operation of businesses. Therefore, this is also an equally important stakeholder.

3. Define security audit and state why you need it

a) Define

A security audit evaluates a company's information system's security systematically by gauging how closely it adheres to predetermined standards. A comprehensive audit often evaluates the security of the system's software, information handling procedures, user behaviour, and physical setup and surroundings.

Security audits are often used to ascertain compliance with laws that stipulate how businesses must handle information, such as the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, and the California Security Breach Information Act.

Along with vulnerability analyses and penetration testing, these audits are one of the three primary categories of security diagnostics. Security audits compare the effectiveness of an information system to a set of standards. An extensive examination of an information system to identify possible security flaws is known as a vulnerability assessment. A security specialist will use a covert technique called penetration testing to check a system's resistance to a particular assault. Each strategy has its own advantages, and the most successful strategy may include combining two or more of them.

b) Why you need it

Prove compliance: There are stringent rules in many businesses. A security audit is evidence that you are adhering to certain standards. Furthermore, certain standards, such as SOC 2, mandate recurring audits.

Reduce risk: Organisations may evaluate and reduce possible threats to their systems and data with the use of security audits. Organisations may take action to stop data breaches, cyberattacks, and other security risks by detecting vulnerabilities and shortcomings.

Lower costs: It may be less expensive to conduct regular security audits than to cope with the fallout after a data breach or cyberattack. Legal fees, reputational harm, and diminished consumer trust are some of the expenses linked to security breaches. More on expenses will be discussed below.

Improve your security posture: Organisations may continually strengthen their security posture with the aid of security audits. Organisations may make sure that their systems and networks are safe and ready to react to any attacks by spotting and fixing new vulnerabilities as they emerge.

4. Recommend the implementation of security audit to stakeholders in an organization

Explain the importance of security audits: Begin by highlighting the importance of security audits and why they are necessary for any organization. Discuss the potential risks and threats that organizations face and how security audits can help to identify and address these issues.

Provide examples of security incidents: Use real-life examples of security incidents that have occurred in other organizations to illustrate the need for a security audit. Discuss the impact that these incidents had on the affected organizations and how they could have been prevented with proper security measures in place.

Emphasize the benefits of a security audit: Discuss the benefits of conducting a security audit, including the identification of potential vulnerabilities and weaknesses, improved security policies and procedures, compliance with regulatory requirements, and overall reduction of the risk of security incidents.

Outline the security audit process: Provide an overview of the security audit process and what it entails. Discuss the different stages of the audit, including planning, data gathering, analysis, reporting, and follow-up.

Highlight the role of stakeholders: Emphasize the importance of stakeholders in the security audit process, including their involvement in planning, data gathering, and follow-up activities.

Discuss the costs and resources required: Finally, discuss the costs and resources required to conduct a security audit. Highlight the potential return on investment and the long-term benefits of investing in security measures.

*REFERENCES:

Acruthers (n.d.) Writing a new policy, *HR Communication Handbook*, [online] Available at: https://kpu.pressbooks.pub/hrcommunication/chapter/writing-a-new-policy/ (Accessed April 27, 2023).

Anon (2020) Risk identification: 7 essentials, *EKU Online*, [online] Available at: https://safetymanagement.eku.edu/blog/risk-identification/#:~:text=Risk%20Identification%20Process%20Steps,risk%20treatment%2C%20and%20risk%20monitoring. (Accessed April 27, 2023).

Anon (2021) What is business continuity?: Vmware glossary, *VMware*, [online] Available at: https://www.vmware.com/topics/glossary/content/business-continuity.html#:~:text=Business%20continuity%20is%20a%20business's,Natural%20disasters (Accessed April 27, 2023).

Anon (2023) What is Data Protection: Principles, strategies & policies: Imperva, *Learning Center*, [online] Available at: https://www.imperva.com/learn/data-security/data-protection/#:~:text=Data%20protection%20is%20the%20process,making%20data%20protection%20increasingly%20important. (Accessed April 27, 2023).

Anon (n.d.) 5-step security risk assessment process, *HackerOne*, [online] Available at: https://www.hackerone.com/knowledge-center/5-step-security-assessment-process (Accessed April 27, 2023).

Anon (n.d.) 8 must-have components of an effective disaster recovery plan, *Arcserve*, [online] Available at: https://www.arcserve.com/blog/8-must-have-components-effective-disaster-recovery-plan (Accessed April 27, 2023).

Anon (n.d.) What is security risk assessment and how does it work?, *Synopsys*, [online] Available at: https://www.synopsys.com/glossary/what-is-security-risk-assessment.html#:~:text=A%20security%20risk%20assessment%20identifies,holistically%E2%80%94from%20an%20attacker's%20perspective. (Accessed April 27, 2023).

Grimmick, R. (2023) What is a security policy? definition, elements, and examples, *Varonis*, Varonis, [online] Available at: https://www.varonis.com/blog/what-is-a-security-policy (Accessed April 27, 2023).

Irwin, L. (2021) Risk terminology: Understanding assets, threats and vulnerabilities, *Vigilant Software - Compliance Software Blog*, [online] Available at: https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities (Accessed April 27, 2023).

Lawler, E. (2019) 5 tips for Creating your security strategy, *TechBeacon*, TechBeacon, [online] Available at: https://techbeacon.com/security/5-steps-evaluate-your-it-security-policy (Accessed April 27, 2023).

Anon (2022) Disaster recovery: 4 key features & building your dr plan, *Cloudian*, [online] Available at: https://cloudian.com/guides/disaster-recovery/disaster-recovery-5-key-features-and-building-your-dr-plan/ (Accessed April 27, 2023).

Anon (n.d.) ISO 31000 principles of risk management — riskoptics - reciprocity, [online] Available at: https://reciprocity.com/iso-31000-principles-of-risk-management/ (Accessed April 27, 2023).

Anon (n.d.) The ISO 31000 risk management process — riskoptics - reciprocity, [online] Available at: https://reciprocity.com/the-iso-31000-risk-management-process/ (Accessed April 27, 2023).