Noureddine Kanzari

ISO/IEC 27001 Lead Auditor

Unlock the Secrets of ISO/IEC 27001 Auditing with Practical Scenarios

Be Prepared for Cybersecurity Challenges

ISO/IEC 27001 Lead Auditor Certification: Your Practical Path to Success

Part 1

Master ISO 27001 Auditing with Real-World Use Cases and Exercises

About the author

Noureddine Kanzari is a cybersecurity expert with an extensive background in IT risk management and cybersecurity instruction. With a diverse range of certifications that includes being a PECB Certified Trainer, EBIOS Risk Manager, ISO 27005 Senior Lead Risk Manager, ISO 27001 Senior Lead Implementer, ISO 27001 Senior Lead Auditor, Cisco Certified Specialist in Security Core and Enterprise Core, NSE4 Network Security Professional, Palo Alto Instructor, Devops Tools Engineer, LPIC-3 Enterprise Professional Security, LPIC-3 Enterprise Professional Virtualization & High Availability, LPIC-2, LPIC-1, Suse Certified Linux Administration, and a Certified Security Auditor in computer security,

Noureddine Kanzari's professional journey is characterized by a series of impactful roles and accomplishments. Throughout his career, he has held various pivotal positions, including:

Chief Information Security Officer (CISO)

Audit Team Leader

Cybersecurity Instructor

Technical Manager

Training Manager

His extensive experience and leadership have contributed significantly to enhancing cybersecurity practices, risk management strategies, and organizational resilience.

Contents

1. Standards and regulatory frameworks

1.1 What is a standard ?

A standard is a document that establishes specific criteria, guidelines, or characteristics for products, processes, services, or systems. Standards are developed to ensure consistency, interoperability, safety, quality, and efficiency in various fields. They serve as a common reference point that can be universally adopted.

Examples :

- ISO/IEC 27001 serves as a standard in the field of information security by providing an approach for organizations to manage and secure information.
- ISO 9001 serves as a standard in the field of quality management. It provide a systematic approach for organizations to establish, implement, maintain, and continually improve a Quality Management System.

Following standards offers a range of benefits :

- **Customer satisfaction and trust building:** Standards provide a set of guidelines and requirements helping organizations produce products and deliver services that meet established benchmarks.
- **Compliance:** Standards often include legal requirements.
- **Risk Management:** Standards provide a structured approach to risk identification, assessment, and management that help organizations mitigate risks effectively.
- **Competitive Advantage:** compliance with certain standards can serve as a competitive advantage. It can differentiate a product or service in the marketplace.
- **Customer Confidence:** Following standards can instill confidence in customers. Knowing that a product or service adheres to recognized standards.
- **Continuous Improvement:** Standards often emphasize the importance of continuous improvement. Organizations that follow standards are encouraged to regularly assess and enhance their processes.

1.2 What is the consequences of not following a standard ?

Not following standards can lead to a variety of consequences, depending on the context and the specific standards involved. Here are some common consequences of not adhering to established standards:

- **Quality Issues:** Failure to follow quality standards may result in products or services that do not meet customer expectations. This can lead to poor quality, customer dissatisfaction, and a negative impact on the organization's reputation.
- **Safety Risks:** Standards often include safety guidelines to protect users, consumers, and workers. Ignoring these standards can lead to safety hazards, accidents, injuries, and legal liabilities.
- **Legal Consequences:** Many industries are subject to regulatory standards, and non-compliance can result in legal consequences, fines, and penalties. Failure to adhere to applicable laws and regulations may lead to lawsuits and damage to the organization's legal standing.
- **Environmental Impact:** Environmental standards are designed to minimize the impact of business activities on the environment. Ignoring these standards can lead to environmental damage, pollution, and violations of environmental regulations, resulting in legal and reputational consequences.
- **Data Breaches and Security Risks:** Ignoring information security standards can expose organizations to the risk of data breaches, cyber-attacks, and unauthorized access. This can lead to the compromise of sensitive information and damage to the organization's reputation.
- **Loss of Customer Trust:** Customers often expect products and services to meet certain standards for quality, safety, and reliability. Failure to meet these expectations can erode customer trust
- **Financial Impact:** Non-compliance with standards can result in financial losses due to legal fees, fines, increased operational costs, and lost business opportunities.
- **Project Failures:** In project management, failure to follow established project management standards can lead to project delays, cost overruns, and ultimately project failure.

Exercie 1 :

Identify and describe two organizations operating in the same industry—one that has successfully implemented ISO 27001 (Information Security Management System) and another that has not. Provide specific examples of how the implementation or lack thereof has influenced each organization's information security posture, customer trust, and overall business performance.

Solution :

Organization A (Implemented ISO 27001) :

- **Security Management System:** Organization A has established and implemented an Information Security Management System (ISMS) in accordance with the requirements of ISO 27001.
- **Risk Assessment and Controls:** A comprehensive risk assessment has been conducted, identifying risks. The organization has implemented a set of controls to mitigate identified risks.
- **Policies and Procedures:** Organization A has documented information security policies and procedures, covering areas such as access control, incident response, encryption, and employee training.
- **Regular Audits and Reviews:** The organization conducts regular internal audits and management reviews to assess the effectiveness of its ISMS.

Consequences and Results:

- **Improved Security Posture:** Organization A experiences a strengthened information security posture. The implementation of ISO 27001 has led to a systematic approach to managing information security risks and has enhanced the overall security resilience of the organization.
- **Enhanced Customer Trust:** Customers and business partners have increased confidence in Organization A's commitment to protecting sensitive information. This trust can lead to increased business opportunities and improved relationships with stakeholders.
- **Compliance with Legal and Regulatory Requirements:** Organization A is more likely to be in compliance with relevant information security laws and regulations, reducing the risk of legal consequences and fines.

- **Efficient Incident Response:** The established incident response procedures enable the organization to respond promptly and effectively to security incidents, minimizing potential damage.

Organization B (Has Not Implemented ISO 27001):

- **Lack of Systematic Security Measures:** Organization B lacks a formalized ISMS and may not have conducted a comprehensive risk assessment. Security measures may be implemented on an ad-hoc basis.
- **Limited Security Policies:** There may be a lack of documented information security policies and procedures, leading to inconsistencies and gaps in security practices.
- **Limited Awareness and Training:** Employees may not receive sufficient training and awareness programs regarding information security best practices.
- **Limited Controls and Monitoring:** The organization may lack systematic controls and monitoring mechanisms for information security.

Consequences and Results:

- **Increased Security Risks:** Organization B is more vulnerable to information security risks due to the lack of a systematic approach. This could result in data breaches, unauthorized access, and other security incidents.
- **Customer Concerns:** Customers and business partners may express concerns about the organization's ability to protect sensitive information. This could lead to a loss of business opportunities and damage to the organization's reputation.
- **Potential Legal Consequences:** The lack of adherence to information security standards may result in non-compliance with legal and regulatory requirements, potentially leading to legal consequences and fines.
- **Inefficiencies and Disruptions:** Without a formalized ISMS, the organization may face operational inefficiencies and disruptions due to security incidents that are not adequately addressed.

Exercise 2:

Evaluation and Improvement of Information System According to ISO 27001

Part 1: Description of XYZ Organization's Information System

Imagine you are tasked with assessing the information system of a fictional organization called XYZ. Briefly describe the context of the information system for this organization by addressing the following questions:

1. **General Overview:** Provide an overview of the XYZ organization's information system. What are its key components and objectives?
2. **Information Assets:** Identify information assets critical to the organization. This may include sensitive data, databases, application systems, etc.
3. **Current Risks:** Identify at least two potential information security risks that the XYZ organization is currently exposed to.
4. **Current Security Measures:** Specify the security measures currently in place to protect information assets. This could include policies, access controls, firewalls, etc.

Part 2: Requirements for ISO 27001 Compliant Improvement

Now, assume that the XYZ organization aims to enhance its information system in compliance with ISO 27001 requirements. Propose specific requirements that the organization should implement to strengthen the security of its information system. Answer the following questions:

1. **Establishment of an ISMS:** Describe the steps the XYZ organization should take to establish an Information Security Management System (ISMS) in line with ISO 27001.
2. **Identification of Sensitive Assets:** What requirements must the organization meet to correctly identify and classify its sensitive information assets?
3. **Risk Assessment:** Propose a method for risk assessment, including probability and impact criteria, to identify and prioritize risks.
4. **Security Policies:** What ISO 27001 requirements should be integrated into the security policies of the XYZ organization?
5. **Training and Awareness:** What measures need to be taken to ensure training and awareness among employees regarding information security?

Solution :

Part 1: Description of XYZ Organization's Information System

1. **General Overview:**
    - XYZ Organization operates in the e-commerce sector, with an extensive online platform for product sales and customer interactions.
    - Key components include a centralized customer database, and a web-based interface for customers and employees.

2. **Information Assets:**

- Critical information assets include customer personally identifiable information (PII), financial transaction records.

3. **Current Risks:**

- Risks include the potential for data breaches leading to the compromise of customer PII.
- Another risk is system downtime due to cyber-attacks, impacting the availability of the e-commerce platform.

4. **Current Security Measures:**

- Current security measures include firewalls, access controls limiting employee access to sensitive data, and periodic security audits.

Part 2: Requirements for ISO 27001 Compliant Improvement

1. **Establishment of an ISMS:**
    - ISO 27001 requires the establishment of an Information Security Management System (ISMS). XYZ should initiate this by conducting a gap analysis to identify existing controls and areas for improvement. They should then develop an ISMS policy, define roles and responsibilities, and establish a risk assessment and management process.

2. **Identification of Sensitive Assets:**

- ISO 27001 mandates the identification and classification of information assets. XYZ should create an inventory of information assets, categorize them based on sensitivity and criticality, and implement controls for secure handling.

3. **Risk Assessment:**

- ISO 27001 requires a systematic risk assessment process. XYZ should conduct a formal risk assessment, considering likelihood and impact, and prioritize risks for mitigation. This involves implementing controls to reduce or eliminate identified risks.

4. **Security Policies:**

- ISO 27001 specifies requirements for security policies. XYZ should develop and implement policies covering areas such as access control, information classification, incident response, and communication security.

1.3. The ISO/IEC 27000 family of standards

The ISO/IEC 27000 family of standards focuses on information security and provides guidelines and international standards for information security management within organizations. These standards are jointly developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

1.3.1. ISO/IEC 27000

ISO/IEC 27000 is designed to provide an introduction and overview of the entire family of information security management system (ISMS) standards. It establishes the vocabulary and framework that sets the stage for understanding and implementing information security management.

Key Components:

Introduction to Key Concepts:

- The standard introduces key concepts related to information security management, such as risk management, controls, ….

Information Security Management Vocabulary:

- ISO/IEC 27000 provides a comprehensive vocabulary for information security management. This includes definitions of terms used throughout the ISO/IEC 27001 series to ensure consistency and clarity.

Relationship with Other Standards:

- The standard outlines the relationship between ISO/IEC 27001 and other relevant standards, including ISO/IEC 27002 (Code of practice for information security controls).

Benefits:

- **Common Understanding:** ISO/IEC 27000 establishes a common understanding of the fundamental concepts and terms related to information security management. This is crucial for organizations seeking to implement and communicate about information security effectively.
- **Basis for Training:** ISO/IEC 27000 serves as a foundational document for training.

Here are some key terms and vocabulary from the ISO/IEC 27000 standard:

1. **Information Security:** Preservation of confidentiality, integrity, and availability of information.
2. **Information Security Management System (ISMS):** A systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability.
3. **Risk:** The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
4. **Risk Assessment:** The overall process of risk identification, risk analysis, and risk evaluation.
5. **Risk Treatment:** The process of selection and implementation of measures to modify risk.
6. **Asset:** Something that has value to the organization, including information and IT infrastructure.
7. **Vulnerability:** Weakness in an asset or control that could be exploited.
8. **Control:** A measure that modifies risk.
9. **Threat:** A potential cause of an unwanted incident that may result in harm to an information system or organization.
10. **Incident:** A single event or a series of related events that have caused harm or have the potential to cause harm to an organization's information system.
11. **Confidentiality:** Ensuring that information is accessible only to those authorized to have access.
12. **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.
13. **Availability:** Ensuring that information is available and usable when needed.
14. **Audit:** Systematic, independent, and documented process for obtaining evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.
15. **Policy:** Overall intentions and direction of an organization related to information security, formally expressed by management.

1.3.2. ISO/IEC 27001

ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The standard is part of the ISO/IEC 27000 family of standards, which covers various aspects of information security.

Key Aspects of ISO/IEC 27001:

1. **Scope Definition (Clause 4):** Organizations define and document the scope of their Information Security Management System (ISMS), specifying what information is covered and the boundaries of the system.
2. **Leadership and Management (Clause 5):** Top management demonstrates leadership and commitment to the ISMS, establishing an information security policy and ensuring its alignment with the organization's strategic direction.
3. **Planning (Clause 6):** This involves risk assessment and treatment, where organizations identify and assess information security risks and then implement controls to manage or mitigate these risks effectively.
4. **Support (Clause 7):** Ensuring the availability of resources, competence, awareness, communication, and documented information necessary to support the operation of the ISMS.
5. **Operation (Clause 8):** The implementation of controls and processes to manage information security risks, including the development and implementation of information security policies and objectives.
6. **Performance Evaluation (Clause 9):** Monitoring, measurement, analysis, and evaluation of the ISMS to ensure its effectiveness and identify opportunities for improvement.
7. **Improvement (Clause 10):** The organization continually seeks opportunities to improve the suitability, adequacy, and effectiveness of the ISMS.

1.3.3. ISO/IEC 27002

ISO/IEC 27002 is a standard that provides guidelines and best practices for implementing and managing information security controls.ISO/IEC 27002 offers a comprehensive set of best practices and controls that organizations can use to address various aspects of information security. It covers a wide range of security domains, providing a framework for developing and maintaining an effective information security management system.

Here are some controls from the ISO/IEC 27002 standard:

1. **Control A.9.2.1: Access Control Policy:** Develop and implement an access control policy.
2. **Control A.9.2.2: User Access Management:** Ensure the management of user access rights is based on business need.
3. **Control A.9.2.3: User Responsibilities:** Clearly define and communicate responsibilities for users to protect their authentication information.
4. **Control A.9.4.1: Information Access Restriction:** Use access controls to restrict access to information systems.

1.3.4. ISO/IEC 27003

ISO/IEC 27003 is a standard that provides guidelines for the implementation of an Information Security Management System (ISMS) based on the requirements specified in ISO/IEC 27001.

Key Components:

1. **Scope Definition:**
   - Guidance on defining the scope of the ISMS, taking into account the organization's business context and the requirements of interested parties.
2. **Leadership and Commitment:**
   - Guidance on the role of top management in providing leadership and commitment to the establishment and continuous improvement of the ISMS.
3. **ISMS Policies:**
   - Guidance on the development and implementation of information security policies and their alignment with the organization's objectives and risk management approach.
4. **Risk Assessment and Treatment:**
   - Guidance on the process of risk assessment and treatment, helping organizations identify and manage information security risks.

5. **Supporting Processes:**
    - Guidance on the establishment and operation of supporting processes for the ISMS, including documentation, communication, and resource management.
6. **Monitoring, Measurement, Analysis, and Evaluation:**
    - Guidance on the processes for monitoring, measuring, analyzing, and evaluating the performance and effectiveness of the ISMS.
7. **Internal Audits:**
    - Guidance on planning, conducting, and managing internal audits of the ISMS to ensure its conformity and effectiveness.
8. **Management Review:**
    - Guidance on the management review process, where top management assesses the performance and effectiveness of the ISMS.
9. **Continuous Improvement:**
    - Guidance on the continual improvement of the ISMS based on the results of monitoring, measurement, analysis, and evaluation, as well as internal audits and management reviews.

Some examples Applications of ISO/IEC 27003:

1. **Scope Definition (ISO/IEC 27003, Section 4):**
    - The organization XYZ conducts a thorough analysis of its business processes, identifying information assets and determining the scope of the ISMS. The guidance in ISO/IEC 27003 helps the Organization XYZ to define the boundaries and applicability of the ISMS.
2. **Leadership and Commitment (ISO/IEC 27003, Section 5):**
    - Top management at the organization XYZ. reviews the guidance on leadership and commitment. They actively engage in the initiation of the ISMS, communicate their commitment to information security, and allocate necessary resources.
3. **ISMS Policies (ISO/IEC 27003, Section 6):**
    - Organization XYZ develops information security policies in line with ISO/IEC 27001 requirements. The guidance in ISO/IEC 27003 helps ensure that the policies are comprehensive, align with the organization's objectives, and are communicated effectively.
4. **Risk Assessment and Treatment (ISO/IEC 27003, Section 7):**
    - Following ISO/IEC 27003 guidance, the organization XYZ establishes a systematic process for identifying and assessing information security risks. They implement controls to treat or mitigate identified risks, aligning with the risk management approach outlined in ISO/IEC 27001.

1.3.5. ISO/IEC 27004

ISO/IEC 27004 is a standard that provides guidelines and general principles for measuring the effectiveness of an Information Security Management System (ISMS) as specified in ISO/IEC 27001.

Key Aspects of ISO/IEC 27004:

1. **Monitoring and Measurement (Clause 6):**
   - Describes the process of monitoring and measuring information security performance and the effectiveness of the ISMS.
2. **Analysis and Evaluation (Clause 7):**
   - Provides guidance on the analysis and evaluation of the monitoring and measurement results, including the assessment of information security performance.
3. **Internal Audit (Clause 8):**
   - Discusses the use of internal audits as a tool for monitoring and measuring the effectiveness of the ISMS.

some examples related to the guidelines provided by ISO/IEC 27004 for monitoring, measurement, analysis, and evaluation of information security performance within an Information Security Management System (ISMS):

1. **Monitoring User Authentication:**
   - **Monitoring Aspect:** Regularly track and log user authentication events, including successful and failed attempts.
   - **Measurement Criteria:** Measure the percentage of successful logins versus unsuccessful logins.
   - **Analysis and Evaluation:** Analyze patterns of failed login attempts to identify potential security threats. Evaluate the effectiveness of authentication controls.
2. **Incident Response Effectiveness:**
   - **Monitoring Aspect:** Monitor and log security incidents as reported or detected.
   - **Measurement Criteria:** Measure the average time taken to respond to and resolve security incidents.
   - **Analysis and Evaluation:** Analyze incident response times to identify bottlenecks or areas for improvement. Evaluate the overall effectiveness of the incident response process.
3. **Patch Management:**
   - **Monitoring Aspect:** Monitor the status of software patches and updates on all information systems.
   - **Measurement Criteria:** Measure the percentage of systems with up-to-date patches.

    - **Analysis and Evaluation:** Analyze the results to identify systems with outdated patches and assess the potential risks. Evaluate the efficiency of the patch management process.
4. **Employee Security Awareness:**
    - **Monitoring Aspect:** Monitor the completion of security awareness training by employees.
    - **Measurement Criteria:** Measure the percentage of employees who have completed security awareness training.
    - **Analysis and Evaluation:** Analyze the training completion rates and assess the impact on the overall security awareness of employees.
5. **Access Control Effectiveness:**
    - **Monitoring Aspect:** Regularly monitor access logs for critical systems and data.
    - **Measurement Criteria:** Measure the frequency and nature of access events.
    - **Analysis and Evaluation:** Analyze access patterns to identify unusual or unauthorized activities. Evaluate the effectiveness of access control mechanisms.
6. **Vulnerability Management:**
    - **Monitoring Aspect:** Continuously monitor and scan the network for vulnerabilities.
    - **Measurement Criteria:** Measure the time taken to patch or mitigate identified vulnerabilities.
    - **Analysis and Evaluation:** Analyze the time-to-patch data to identify areas for improvement. Evaluate the efficiency of the vulnerability management process.

Examples of Incident Response Effectiveness:

- The organization aims to keep false positives below 5% of total incidents
- mitigations are expected to be successful in at least 95% of cases
- Documentation completeness is targeted at 80% of incidents
- User satisfaction with the incident response process is expected to be at least 85%

1.3.6. ISO/IEC 27005

ISO/IEC 27005 is a standard that provides guidelines for information security risk management.

Key Components:

1. **Context Establishment (Clause 4):**
    - Understanding the organization's context and the objectives and constraints of information security risk management.
2. **Leadership and Commitment (Clause 5):**
    - Ensuring leadership commitment to information security risk management and integrating it into the overall governance framework.
3. **Integration with the Organization's Governance Framework (Clause 6):**
    - Integrating information security risk management into the organization's governance framework and ensuring alignment with strategic objectives.
4. **Risk Assessment Process (Clause 7):**
    - Defining a risk assessment process that includes risk identification, risk analysis, and risk evaluation.
5. **Risk Treatment Process (Clause 8):**
    - Establishing a risk treatment process that includes risk treatment options, selecting and implementing risk treatments, and monitoring and reviewing the effectiveness of treatments.
6. **Monitoring and Review of the Risk Assessment and Risk Treatment Framework (Clause 9):**
    - Establishing processes for monitoring and reviewing the risk assessment and risk treatment framework to ensure ongoing effectiveness.

Example of application ISO 27005: Small E-commerce Business

Context: A small e-commerce business operates an online store where customers make purchases, and sensitive information such as credit card details is processed.

Application of ISO/IEC 27005:

1. **Risk Identification:**
   - Identify risks related to online transactions, data breaches, and potential attacks on the e-commerce platform.
2. **Risk Analysis:**
   - Assess the likelihood and potential impact of a data breach, considering factors such as the number of transactions, the sensitivity of customer data, and the adequacy of current security measures.
3. **Risk Evaluation:**
   - Determine which risks pose the highest threats to the business and need immediate attention. For example, the risk of a payment processing system vulnerability might be prioritized.
4. **Risk Treatment:**
   - Implement measures to mitigate identified risks, such as enhancing encryption protocols, regularly updating security patches, and conducting security awareness training for employees.
5. **Monitoring and Review:**
   - Regularly monitor (Audit, metrics such as the reduction in the number of security incidents, incident report), review emerging threats, and adjust the risk management strategy accordingly.

1.3.7. ISO/IEC 27006

ISO/IEC 27006 is a standard that provides requirements and guidance for organizations conducting audits and certifications of Information Security Management Systems (ISMS) based on the ISO/IEC 27001 standard.

Key Components:

1. **Requirements for Bodies Providing Audit and Certification of ISMS (Clauses 4-10):**
    - Establishes detailed requirements for certification bodies
2. **Covers areas such as competence, impartiality, audit process**
3. **Auditor Competence (Clause 7):**
    - Specifies requirements for the competence of auditors engaged in the assessment of ISMS.
4. **Impartiality (Clause 8):**
    - Defines the principles and requirements for ensuring the impartiality of certification bodies during the certification process.
5. **Audit Process (Clause 9):**
    - Outlines the stages and activities involved in the audit process, including the planning, conduct, and reporting of ISMS audits.
6. **Issue and Maintenance of Certificates (Clause 10):**
    - Describes the requirements for the issuance and maintenance of ISO/IEC 27001 certificates.
7. **Confidentiality (Clause 11):**
    - Specifies requirements related to confidentiality in the audit and certification process.
8. **Management of Competence (Clause 12):**
    - Details the requirements for the certification body to ensure ongoing competence of its personnel

Example : Certification Process for Company A

Company A is seeking ISO/IEC 27001 certification for its Information Security Management System. Here's how ISO/IEC 27006 would be applied:

1. **Choosing a Certification Body :**
    - Company A selects a certification body that adheres to ISO/IEC 27006. The certification body must demonstrate competence, impartiality, and compliance with ISO/IEC 27006 requirements.
2. **Audit Planning:**
    - The certification body plans the ISMS audit, considering the scope and objectives of Company A's ISMS. This includes determining the audit team, audit duration, and necessary resources.
3. **Auditor Competence:**
    - The certification body ensures that auditors assigned to Company A's audit possess the necessary competence. This includes relevant knowledge and skills in information security.
4. **Impartiality:**
    - The certification body maintains impartiality throughout the certification process, ensuring that there are no conflicts of interest that could compromise the objectivity of the audit.
5. **Audit Process:**
    - The audit team conducts an assessment of Company A's ISMS against the requirements of ISO/IEC 27001. This involves evaluating policies, processes, risk management practices, and other elements.
6. **Issue and Maintenance of Certificates:**
    - If Company A's ISMS is found to be in compliance with ISO/IEC 27001, the certification body issues a certificate. The certification body is responsible for maintaining the validity of the certificate through regular surveillance and recertification audits.

1.3.8. ISO/IEC 27007

ISO/IEC 27007 provides guidelines for the effective, efficient, and consistent auditing of ISMS, particularly in the context of ISO/IEC 2700. ISO/IEC 27007 is designed to be used in conjunction with ISO/IEC 27001. It provides guidance on the principles of auditing, managing an audit program, conducting management system audits, and evaluating the competence of individuals involved in the audit process.

1. **Audit Principles:**

- The standard outlines fundamental audit principles, including the need for independence, ethical conduct, and systematic and disciplined approaches to auditing.

2. **Audit Program Management:**

- ISO/IEC 27007 provides guidance on establishing and maintaining an audit program, considering factors such as the objectives, scope, frequency, and methods of audits.

3. **Competence and Evaluation:**

- It addresses the competence requirements for personnel involved in the audit process and provides guidance on evaluating the effectiveness of the audit process.

4. **Audit Activities:**

- The standard covers various aspects of audit activities, including initiating the audit, preparing audit activities, conducting audit activities, and concluding and reporting the audit.

5. **Documentation:**

- Guidelines are provided for documenting audit activities, including the audit plan, audit records, and audit findings.

6. **Audit Reporting:**

- ISO/IEC 27007 offers guidance on preparing and presenting audit reports, ensuring that relevant information is communicated to relevant stakeholders.

7. **Follow-Up Audits:**

- The standard includes recommendations for conducting follow-up audits to verify the implementation and effectiveness of corrective actions.

1.4. ISO/IEC 27001 benefits

Implementing ISO 27001, the international standard for information security management systems (ISMS), offers several benefits to organizations. Here are some concrete examples of the benefits derived from ISO 27001 implementation:

1. **Enhanced Information Security:**
   - **Example:** An organization that implements ISO 27001 establishes a robust framework for managing information security risks. This could include encrypting sensitive data, implementing access controls, and regularly updating security measures.
2. **Risk Management:**
   - **Example:** Through risk assessments and risk treatment plans mandated by ISO 27001, organizations can identify potential threats and vulnerabilities. For instance, an e-commerce company might identify the risk of a data breach and implement measures to mitigate this risk, such as regular security audits and penetration testing.
3. **Legal and Regulatory Compliance:**
   - **Example:** Many industries are subject to data protection and privacy laws. ISO 27001 helps organizations comply with these regulations. For instance, a healthcare organization might align its information security practices with ISO 27001 to ensure compliance with healthcare data protection laws.
4. **Improved Customer Trust:**
   - **Example:** A cloud service provider obtaining ISO 27001 certification can assure its customers that it follows international best practices for securing their data. This can significantly enhance customer trust, leading to increased business opportunities.
5. **Competitive Advantage:**
   - **Example:** In competitive industries, ISO 27001 certification can serve as a differentiator. For example, a software development company may win more contracts by demonstrating its commitment to information security through ISO 27001 certification.
6. **Efficient Incident Response:**
   - **Example:** ISO 27001 requires organizations to establish an incident response plan. In the event of a security incident, a financial institution with ISO 27001 certification might respond more efficiently, minimizing the impact on operations and customer trust.
7. **Cost Savings Through Efficiency:**
   - **Example:** By systematically identifying and addressing risks, organizations can prevent costly security incidents. For example, a manufacturing company might prevent the loss of intellectual property by implementing controls outlined in ISO 27001.
8. **Employee Awareness and Training:**
   - **Example:** ISO 27001 emphasizes the importance of employee awareness and training in information security. An organization might conduct regular training sessions to educate employees about phishing

threats, thereby reducing the risk of security breaches caused by human error.

9. **Continuous Improvement:**
    - **Example:** ISO 27001 requires organizations to continually monitor and improve their information security management system. An online retailer might regularly update its security policies and procedures based on the evolving threat landscape, ensuring ongoing effectiveness.
10. **Global Recognition:**
    - **Example:** ISO 27001 is recognized internationally. A multinational corporation can achieve consistent information security standards across its locations worldwide, facilitating global operations and collaborations.
11. **Supplier and Partner Relationships:**
    - **Example:** Organizations may require their suppliers and partners to comply with ISO 27001 standards, creating a secure ecosystem. A technology company might choose suppliers who have also implemented ISO 27001, ensuring a secure supply chain.

Exercice 3

Context of the organization:

- Organization A operates in the technology sector and deals with sensitive client data.
- The company is expanding its client base, leading to an increase in the volume of confidential information it manages.
- There is a growing concern about the potential risks and threats to information security, including data breaches and unauthorized access to proprietary software.

Your Task:

1. Identify the potential information security challenges that the organization might face.
2. Define and explain five benefits of implementing ISO 27001 that are specifically relevant to addressing the challenges faced by the organization.
3. Provide concrete examples or scenarios to illustrate how each benefit contributes to the improvement of information security practices within TechSecure.

Solution :

Benefits of ISO 27001 Implementation:

1. Enhanced Information Security:

- **Definition:** Implementing ISO 27001 will enhance the information security by establishing a systematic approach to identify, manage, and mitigate information security risks. This includes implementing measures such as access controls, encryption, and regular security audits.
- **Example/Scenario:** Suppose the organization identifies a potential vulnerability in its software development environment through a risk assessment. With ISO 27001, the company can systematically address this vulnerability by implementing enhanced access controls and encryption measures, thereby minimizing the risk of unauthorized access and data breaches.

2. Legal and Regulatory Compliance:

- **Definition:** ISO 27001 helps the company comply with relevant laws and regulations related to information security, especially in the tech sector. This includes compliance with data protection and privacy laws.
- **Example/Scenario:** Given the increasing stringency of data protection laws, ISO 27001 ensures that the organization has comprehensive policies and controls in place. For instance, the standard helps the company align with the General Data Protection Regulation (GDPR) by implementing measures such as data encryption.

3. Improved Customer Trust:

- **Definition:** ISO 27001 certification can significantly improve customer trust by demonstrating a commitment to information security. This is crucial for a technology company handling sensitive client data.
- **Example/Scenario:** The company, after obtaining ISO 27001 certification, can showcase this achievement in its marketing materials and communications. This transparent approach enhances customer confidence, assuring clients that their data is handled with the utmost security measures in place.

4. Cost Savings Through Efficiency:

- **Definition:** ISO 27001 contributes to cost savings by preventing security incidents and addressing risks efficiently. Proactive risk management and prevention measures can save costs associated with data breaches or system downtime.
- **Example/Scenario:** Imagine the organization identifies a potential risk related to outdated security protocols through an ISO 27001 audit. By promptly updating these protocols, the company avoids a potential data breach, saving

significant costs associated with incident response, legal consequences, and reputational damage.

5. Continuous Improvement:

- **Definition:** ISO 27001 emphasizes a culture of continuous improvement in information security practices. This is essential for evolving landscape where new threats emerge regularly.
- **Example/Scenario:** The company regularly reviews its information security policies and procedures based on the results of internal audits and changes in the threat landscape. For instance, the company might adapt its incident response plan to address emerging cybersecurity threats, ensuring continuous improvement and resilience against evolving risks.

2. The ISO/IEC 27001 Audit process

The ISO 27001 audit process involves several phases, including setting up the Information Security Management System (ISMS), conducting internal audits, selecting the certification body, preparing for the certification audit, and completing the audit phases to obtain the ISO 27001 certificate. Here is a detailed breakdown of the ISO 27001 audit process:

2.1. Setting up the Information Security Management System (ISMS)

- **Define Scope and Objectives:** Determine the scope and objectives of the ISMS, specifying what information assets are to be protected and the desired security outcomes.
- **Risk Assessment:** Conduct a risk assessment to identify vulnerabilities, threats, and associated risks.
- **Risk Treatment:** Develop and implement a risk treatment plan to mitigate identified risks through security controls.
- **ISMS Documentation:** Document the ISMS framework, including security policies, procedures, and controls.

2.2. Internal Audit

- **Internal Audit Planning:** Plan internal audits based on the defined scope and objectives of the ISMS.
- **Audit Execution:** Conduct internal audits to evaluate the effectiveness of the ISMS. This includes reviewing documented processes and controls, interviewing personnel, and performing tests.
- **Audit Reports:** Prepare audit reports that detail findings, non-conformities, and improvement opportunities.
- **Corrective Actions:** Implement corrective actions to address non-conformities and improve the ISMS.

2.3. Selection of Certification Body

- **Choose a Certification Body:** Select a reputable and accredited certification body that will assess your ISMS against ISO 27001 requirements.
- **Contract and Agreement:** Establish a contract or agreement with the certification body to initiate the certification audit process.

2.4. Stage 1 Audit

- **Document Review:** The certification body reviews the ISMS documentation to assess its completeness and alignment with ISO 27001.

  The certification body auditors will carefully review the documentation provided by the organization. This documentation typically includes policies,

procedures, work instructions, records, and evidence of the organization's ISMS.

The certification body will pay particular attention to:

- The organization's Information Security Policy.
- The Statement of Applicability (SoA) that details the selected security controls.
- Risk assessment and treatment documentation.
- Records of internal audits and management reviews.
- Documentation related to the organization's security controls and their implementation.

The organization's Access Control Policy and associated documents would be subject to review during this phase.

Document: Access Control Policy

- The auditors would assess whether the Access Control Policy aligns with ISO 27001 requirements. This includes verifying that the policy outlines access control objectives, responsibilities, and the management's commitment to access control.

Document: Access Control Procedures

- The auditors would review documented procedures to ensure that they are in place and that they provide specific instructions on how access control is implemented.

Evidence: Access Control Implementation

- The certification body may request evidence of access control measures, such as access logs, user account management records, and security incident reports.

- **Assessment of Preparedness:** The audit team evaluates the organization's readiness for the certification audit.
- **Non-Conformities Identification:** Any non-conformities or deviations from ISO 27001 requirements are identified.

The auditors will verify the completeness of the documentation by ensuring that it addresses all relevant aspects of ISO 27001 requirements. Completeness may be verified by comparing the documentation to a checklist of ISO 27001 clauses and controls. If the auditors identify any discrepancies, omissions, or non-conformities in the documentation, these will be documented as findings. The organization will be required to address these findings before proceeding to the certification audit.

2.5. Stage 2 Audit

- **On-Site Audit:** The certification body conducts an on-site audit to assess the implementation and effectiveness of the ISMS.
- **Testing Controls:** The auditors examine the application of security controls and gather evidence to confirm their effectiveness.
- **Audit Findings:** Non-conformities or findings may be identified during the audit.

Example: Access Control in Stage 2 Audit

1. Review of Access Control Implementation:

- Auditors will select a critical area to evaluate, such as access control. This includes assessing whether access to sensitive systems and data is adequately controlled. Auditors will review access control policies, procedures, and evidence of their implementation.

2. Evaluation of Security Controls:

- Auditors will evaluate the effectiveness of security controls related to access control. For instance, if the policy states that employees must use multi-factor authentication (MFA) to access the organization's systems, auditors will check whether MFA is indeed implemented.
- **Concrete Steps:**
    - Auditors may interview employees or IT staff to confirm their use of MFA.
    - They will review access logs and records to ensure that MFA is enforced during system access.
    - Auditors might randomly select a few user accounts and validate that MFA is in place and properly functioning.

3. Testing of Incident Response:

- Auditors may simulate a security incident or breach scenario to test the effectiveness of the incident response plan. For example, they might send a simulated phishing email and assess the organization's ability to detect and respond to it.
- **Concrete Steps:**
    - Auditors will assess whether the incident is detected promptly.
    - They will evaluate the organization's response procedures, including incident reporting, containment, and recovery.
    - They may also analyze the effectiveness of corrective actions taken to prevent future incidents.

4. Review of Security Awareness and Training:

- Auditors will evaluate the security awareness and training program by reviewing training records and conducting interviews with employees.
- **Concrete Steps:**
  - They may interview employees to assess their awareness of security policies and their understanding of security best practices.
  - Auditors will review training records to verify that employees have received appropriate security training.

5. Verification of Compliance:

- Auditors will confirm that the organization's security practices are aligned with ISO 27001 requirements and the ISMS's Statement of Applicability (SoA).

6. Assessment of Incident Reporting:

- Auditors will evaluate the organization's incident reporting and investigation process. They will assess how incidents are documented, reported, and resolved.

7. Sampling and Observation:

- Auditors may randomly sample security incidents, access requests, or other relevant data. They may also observe the behavior of employees to assess their compliance with security policies and procedures.

2.6. Obtaining the Certificate

- **Report and Certification:** The certification body compiles an audit report, which includes audit findings, non-conformities, and the status of the ISMS.
- **Decision:** Based on the audit findings, the certification body makes a decision on whether to issue the ISO 27001 certificate.
- **Certificate Issuance:** If the organization meets the requirements, the ISO 27001 certificate is issued, signifying compliance with the standard.

Example of Audit Report for ISO 27001 Certification Audit :

Audit Date: [Date of the Audit]

Auditors: [Names of Audit Team Members]

Organization: [Name of the Audited Organization]

Audit Scope: [Scope and Objectives of the Audit]

Executive Summary: The ISO 27001 certification audit was conducted to assess the effectiveness of [Organization's Name] Information Security Management System (ISMS). The audit focused on evaluating the organization's compliance with ISO 27001 requirements, the implementation of security controls, and the management of information security risks.

Audit Findings:

Non-Conformity 1: Access Control

- **Description:** The organization's Access Control Policy specifies the use of multi-factor authentication (MFA) for accessing sensitive systems. However, during our assessment, we identified instances where MFA was not consistently enforced.
- **Recommendation:** The organization should review and strengthen its MFA implementation and ensure that all users accessing sensitive systems adhere to this control.

Non-Conformity 2: Incident Response

- **Description:** The incident response plan was tested through a simulated phishing attack. While the incident was detected, the response procedures lacked clarity and prompt execution.
- **Recommendation:** The organization should refine its incident response procedures and ensure that the response team is adequately trained and equipped to respond effectively to security incidents.

Non-Conformity 3: Security Awareness Training

- **Description:** Although the organization provides security awareness training, there was inconsistent documentation of employee participation. Some employees lacked records of completed security training.
- **Recommendation:** The organization should maintain complete and up-to-date records of security awareness training for all employees to ensure comprehensive coverage.

Status of the ISMS: Overall, [Organization's Name] has demonstrated a commitment to information security and has established a robust ISMS foundation. While some non-conformities were identified during the audit, it is important to note

that these findings present opportunities for improvement and do not detract from the organization's dedication to information security.

Recommendations:

- [Organization's Name] should take prompt corrective actions to address the identified non-conformities and strengthen its security controls.
- The organization should conduct a thorough review of its ISMS documentation to ensure consistency and alignment with ISO 27001 requirements.
- It is advisable for the organization to conduct additional internal audits to proactively identify and address potential non-conformities before the certification audit's next stage.
- [Organization's Name] is encouraged to maintain a culture of continuous improvement and information security awareness to enhance its ISMS.

We recommend that [Organization's Name] proceed with the implementation of corrective actions to address the identified non-conformities. These actions should be taken promptly and in accordance with the organization's internal procedures.

Upon successful corrective action implementation, we recommend that the certification body review and confirm the resolution of non-conformities before issuing the ISO 27001 certificate to [Organization's Name].

3. Information & Assets

3.1. Information

Are often given higher protection priority due to their direct impact on the organization's success and continuity.

Example:

Customer database: It directly contributes to the bank's core business (managing customer accounts)

Contracts and Agreements: Legal agreements with customers, partners, and suppliers

Innovation Roadmaps: Plans for introducing new products, technologies

Business Plans: Long-term and short-term strategies for growth, expansion, and development

Equipment and Machinery: Technical specifications, maintenance schedules, and operational guidelines

Electronic Health Records: store patient medical histories, lab results

Formulas and Designs: give the company a competitive edge.

Student Data: Information about students

Sales Process: This process involves selling products to customers

Customer Service Process: This process focuses on addressing inquiries, issues, and complaints

3.2. Asset

Hardware Assets

- ***Servers:*** Physical machines that host applications
- ***Desktop Computers***: Standard workstations
- ***Laptops***: Portable computers
- ***Storage Devices:*** Devices for storing data, such as hard drives, (NAS) systems
- ***Printers and Scanners:*** Devices for printing and scanning documents

Software Assets

- ***Operating Systems:*** Software that manages hardware. Example Windows 10
- ***Applications:*** example Microsoft Office
- ***Security Software:*** Tools for antivirus, anti-malware, and firewall protection
- ***Development Tools:*** Software for programming and software development, examples Visual Studio
- ***Database:*** Software for creating, maintaining, and querying databases. Example Oracle Database, MySQL, Microsoft SQL Server

Network Assets

- ***Network Cables:*** Ethernet, fiber optic, ..
- ***Wireless Access Points:*** Devices that enable wireless network connectivity
- ***Routers and Switches:*** Devices that direct data traffic on a network

Security Assets

- ***Firewalls:*** Devices or software that protect networks from unauthorized access.
- ***Intrusion Detection/Prevention Systems (IDS/IPS):*** Tools that monitor and analyze network traffic for potential security breaches
- ***Encryption Tools:*** Software for encrypting data to ensure confidentiality. Example OpenSSL

Human Assets:

- ***Software Developer:*** Creates, tests, and maintains software applications. Examples: Java Developer
- ***Web Developer:*** Specializes in creating websites
- ***System Administrator:*** Manages and maintains an organization's IT infrastructure
- ***Database Administrator:*** Manages and maintains databases
- ***Chief Information Officer (CIO):*** responsible for aligning IT with the organization's goals
- ***Information Security Analyst:*** Protects an organization's data and information systems from security breaches

Relationship: Information / asset (Hardware/Software/Network/Personnel)

Information	Description	Responsible	Asset	Description
Customer Information	Personal and financial data of customers	HR	Customer Database	This database holds all the customer-related data. It includes sensitive details such as names, addresses, contact information, purchase history, and possibly payment information. The database requires robust security measures to prevent unauthorized access or data breaches
			Application Server	The application server hosts the software applications used to manage and process customer information. It may also handle authentication and authorization, ensuring only authorized personnel can access the data
			Network Infrastructure	The network infrastructure connects all components and enables data flow between them. It includes routers, switches, firewalls, and other

				network devices. Securing the network is crucial to prevent unauthorized access and data interception
			Storage Systems	These systems store the data, including the customer information. Proper encryption, access controls, and backup strategies are essential to protect against data loss and unauthorized access
			Communication Systems	Facilitating real-time communication among quality control stakeholders

4. Vulnerability, threat, impact

4.1. vulnerability

The vulnerability refers to a weakness in an information technology (IT) system, software application, network infrastructure, or any digital asset that could be exploited by malicious actors to compromise the confidentiality, integrity, or availability of data, services, or resources.

These weaknesses are often targeted by cybercriminals, hackers, or malicious software (malware) to gain unauthorized access, steal sensitive information, launch attacks, or cause damage to IT systems and assets.

Here are some common IT vulnerabilities:

- Unpatched Software
- Misconfigured Cloud Services
- Weak Passwords
- Inadequate Access Controls
- Outdated Software
- Lack of Encryption
- Flaws in software code
- Lack of network segmentation
- Lack of physical access controls
- Inadequate Backup
- Weak data loss prevention
- Inadequate Monitoring and Logging
- Default Configurations
- ….

4.2. Threat

Malware:

malicious software designed to disrupt, damage, or gain unauthorized access.

Example: A company employee receives an email with an attachment claiming to be an invoice. Once the attachment is opened, it releases a ransomware virus that encrypts all the files.

Phishing:

involves sending fraudulent emails that appear to be from a legitimate source, aiming to trick recipients into revealing sensitive information or clicking on malicious links.

Example: A bank customer receives an email that appears to be from their bank, asking them to click on a link to update their account information due to a security breach. The link takes them to a fake website that collects their login credentials, allowing the attacker to access their bank account.

Denial of Service (DoS) Attack:

A DoS attack floods a network with excessive traffic, overwhelming its resources and causing it to become unavailable to users.

Example: saturate servers, making a website inaccessible to customers during a major sales event.

Data Breach:

Involves unauthorized access to sensitive or confidential information, potentially leading to its theft, exposure, or misuse.

Example: A healthcare organization's database containing patient records is breached by hackers. The attackers steal personal health information, including names, addresses, medical histories, and social security numbers, which are later sold on the dark web.

Insider Threat:

Individuals within an organization who misuse their access privileges to compromise security.

Example: A disgruntled employee with administrative access to the company's systems intentionally leaks proprietary information to a competitor, causing financial harm and loss of competitive advantage.

Man-in-the-Middle (MitM) Attack:

An attacker intercepts communications between two parties without their knowledge.

Example: An attacker sets up a fake Wi-Fi hotspot in a public place, tricking users into connecting to it. All data transmitted through this hotspot is intercepted and monitored by the attacker, potentially compromising sensitive information.

Social Engineering:

Involves manipulating individuals to divulge confidential information or perform actions that compromise security.

Example: An attacker poses as a technical support representative and calls an employee, claiming there is a critical issue with their computer. The attacker convinces the employee to provide their login credentials, which are then used to gain unauthorized access to the company's systems.

Zero-Day Exploit:

Targets a vulnerability in software before the software's developer releases a fix or patch.

Example: A hacker discovers unknown vulnerability in a web browser and develops an exploit to take advantage of it. They use the exploit to gain unauthorized access to users' computers and steal sensitive data.

Theft of Hardware:

Losing essential hardware could disrupt the business operations, compromise sensitive data, and lead to financial losses.

Example: the thief enters the office and quickly snatches the laptop before anyone notices. The stolen laptop contains sensitive company data, confidential reports, and customer information.

Destruction of equipment:

Depending on the extent of the destruction, the company could face data loss if backups were stored on-site and were also affected by the attack.

Example: The attacker successfully gains unauthorized physical access to the company's data center. They proceed to physically damage servers, network switches, and storage devices, causing a significant disruption in the company's operations.

SQL injection:

The website's login form is vulnerable to SQL injection due to poor input validation.

Example:

User enters his username: john_doe

User enters his password: mysecretpassword

The application constructs an SQL query to check if the provided credentials exist in the database:

SELECT * FROM users WHERE username = 'john_doe' AND password = 'mysecretpassword';

A malicious user enters the following username: ‘john_doe' OR '1'='1' --‘

For the password, the malicious usercan enter anything or leave it blank

The application constructs the SQL query:

SELECT * FROM users WHERE username = 'john_doe' OR '1'='1' --' AND password = '';

In this case, the -- is a comment in SQL, causing the rest of the query (including the password check) to be ignored.

The query will always return true because '1'='1' is always true in SQL

As a result, the attacker gains access to the account associated with the username john_doe, even without knowing the correct password.

Brute Force Attack:

An attacker decides to target an account usinga combination of a username and password.

Example: The attacker uses automated software or scripts to generate a wide range of possible password combinations. These combinations may include common passwords, dictionary words, character variations, and different lengths of passwords.

Intercepting sensitive data in transit:

Unauthorized individual capturing and accessing sensitive information while it is being transmitted over a network.

Example: set up a rogue Wi-Fi hotspot with a similar name to the coffee shop's legitimate network. Unsuspecting users might accidentally connect to this rogue hotspot, thinking it's the official network, all the data transmitted over this rogue network is intercepted by the attacker. This includes login credentials, account numbers, and other sensitive information.

USB-Based Threats:

Refer to security risks and vulnerabilities that can arise from the use of USB (Universal Serial Bus) devices, such as USB flash drives, external hard drives.

Example: an employee at a large corporate office finds a USB flash drive lying in the parking lot. Curious about its contents, the employee plugs the USB drive into his office computer to see what's on it. Unbeknownst to them, the USB drive contains malicious software designed to infiltrate the corporate network. When the infected USB drive is plugged into the computer, the malicious software executes a code that exploits a vulnerability in the operating system. The malware spreads across the internal network, scanning for other vulnerable computers and devices connected to the network. The malware steals sensitive data, including proprietary information, customer data, and employee credentials

DNS poisoning:

Malicious user changes the records that a server uses to direct traffic to the right websites. This can cause the DNS server to return the wrong IP address for a given domain name, redirecting traffic intended for a legitimate website to the attacker’s website.

Example: a customer of a bank, frequently access the online banking portal to manage his account. In a normal DNS Resolution, he types in the bank's URL (e.g., www.examplebank.com), his computer sends a DNS query to a DNS server to resolve the domain name into an IP address.

In DNS Cache Poisoning: An attacker, through various means, manages to manipulate the DNS response that the computer receives from a compromised DNS server. The attacker's goal is to insert a malicious IP address mapping for the bank's domain. The computer's DNS cache now contains the malicious IP address for the bank's domain. When the user attempts to access the bank's website, his browser is redirected to a fraudulent website that closely resembles the real online banking portal.The fake banking website prompts to enter the login credentials and other sensitive information. Unaware of the attack, the user provide his username and password.

Botnets:

A botnet is a network of compromised computers, also known as "bots" or "zombies," that are under the control of a malicious actor. These compromised computers are typically infected with malware, allowing the attacker to remotely control them and use their combined power to carry out various cyberattacks. One of the most common uses of botnets is to launch Distributed Denial of Service (DDoS) attacks.

Example: The attacker infects a large number of computers around the world with malware, turning them into bots. These infected computers become part of the botnet and are under the attacker's remote control. The attacker uses a Command and Control (C&C) server to manage and coordinate the actions of the botnet. This server sends instructions to the infected computers, telling them when and how to launch the attack. The attacker selects a target, which could be a website, an online service, or an organization's network. The choice of target might be motivated by financial gain, political reasons. The C&C server sends commands to the infected computers, instructing them to flood the target with a massive volume of traffic. This flood of traffic overwhelms the target's resources, such as its bandwidth, processing power, and memory.

Fake Software:

A fake software contains hidden malware.

Example: A company purchases what it believes to be genuine software licenses from the third-party vendor. The counterfeit software is installed across various departments within the organization, including critical financial systems. Unbeknownst to the company, the fake software contains hidden malware designed to steal sensitive financial data and credentials. The malware activates, infiltrating the company's network, capturing sensitive customer financial data, employee login credentials, and other confidential information.

DHCP Starvation:

An attacker floods the DHCP server with a large number of DHCP requests, depleting the pool of available IP addresses and causing legitimate devices to be unable to obtain addresses.

Example: A corporate network uses DHCP to assign IP addresses to computers, printers, and other devices.The DHCP server has an address pool of 100 IP addresses to assign. An attacker connects a rogue device (like a laptop) to the network.The attacker configures the rogue device to send a high volume of DHCP requests to the DHCP server, requesting new IP addresses.The rogue device keeps requesting IP addresses in rapid succession, exhausting the DHCP server's available IP addresses.

Fraud:

Manipulation, or misrepresentation for financial gain or other malicious purposes. It encompasses a wide range of tactics and techniques aimed at unlawfully obtaining money, sensitive data, or other valuable assets.

Example: The attacker poses as the executive and sends convincing emails to other employees, clients, or vendors, instructing them to make financial transactions. The attacker might send an email to the finance department requesting an urgent transfer to a fraudulent account. Since the email appears to come from a trusted source, the recipient may follow through with the instructions.

Rogue DHCP Servers:

Unauthorized DHCP servers introduced into the network can assign incorrect or malicious network settings to devices, potentially redirecting traffic to attacker-controlled servers.

Example: The network is set up with a legitimate DHCP server that assigns IP addresses and network configuration to all devices on the network. However, an attacker with malicious intentions manages to connect a rogue device to the LAN. This rogue device has been configured to act as a DHCP server and is designed to distribute IP addresses to other devices on the network. The attacker's goal is to intercept and manipulate network traffic, potentially stealing sensitive information. The rogue device, being a deceptive DHCP server, responds to these DHCP discovery requests with its own DHCP offers. It assigns IP addresses and provides malicious network settings, such as incorrect DNS server addresses or gateway information.

Privilege Escalation:

Is a cybersecurity threat where an attacker exploits vulnerabilities in a system or application to gain higher levels of access and control than they are initially authorized for.

Example: A corporate network with different user roles and access levels. There are regular employees, managers, and administrators, each with varying levels of access to sensitive data and critical systems. The attacker gains initial access to the network by exploiting a known vulnerability in an outdated web server that the company failed to patch. The attacker starts as a regular employee with limited access to company resources. Through careful exploration and exploitation, he discovered a vulnerability in a file-sharing system used by employees to collaborate on projects. By exploiting this vulnerability, the attacker manages to gain access to a manager's account. He continuied to search for vulnerabilities and weaknesses. Eventually, he finds a misconfigured server that allows to execute arbitrary commands with elevated privileges.

Input error:

Refers to a situation where incorrect data is entered into a system or application.

Example: a financial institution that offers online banking services to its customers. Users can transfer money between accounts. A customer intends to transfer $100 from his savings account to his checking account. However, he accidentally input "$1000" instead of "$100" due to a typographical error.

Departure of key person:

A company heavily reliant on the expertise and leadership of the Chief Technology Officer (CTO), who has been instrumental in driving innovation and overseeing crucial development projects. The CTO possesses extensive knowledge about the company's proprietary technologies, trade secrets, and strategic plans. His departure could potentially lead to the loss of critical intellectual property. Competitors or other organizations might try to capitalize on this opportunity.

Alteration of information:

Refers to the unauthorized modificationof data, records with the intent to manipulate, or cause harm.

Example: A malicious actor targets a financial institution's database with the intention of altering account balances and transaction records. The attacker gains unauthorized access to the financial institution's internal network through a phishing email that tricks an employee into clicking on a malicious link. Once inside the

network, the attacker conducts reconnaissance to identify critical databases. The attacker locates the database containing account balances and transaction records. He uses his access to modify the account balances. To avoid detection, the attacker modifies log files and access records to erase any evidence of his activities.

Repudiaion:

Repudiation is an IT threat that occurs when a user denies performing a particular action or transaction.

Example: The user logs into his online banking account and transfers $1,000 to his friend as a birthday gift. After a few days, the user denies making the $1,000 transfer and claims that he never initiated or authorized the transaction.

4.3. Threat/vulnerability relationship

The following table illustrates the relationship between various elements within a security context: threats, their sources, associated objectives, exploited vulnerabilities, and the corresponding impacted assets :

Threat	Source	Source description	Target objective	Exploited Vulnerabilty	Affected assets
Malware	Hacker	Individual with malicious intent create and distribute malware	° Steal sensitive information ° Gain unauthorized access ° Cause damage	°No awareness : Malware creators often rely on tricking users into performing actions that aid in the installation of malware, such as clicking on malicious links, downloading infected attachments, or disclosing sensitive information °Misconfiguration: Malware can exploit weaknesses in network configurations or protocols to spread laterally within an organization's infrastructure °Not patched software: Malware can leverage these exploits to gain access before a patch is released °Weak Authentication: Malware may target weak passwords or default credentials to gain access to systems °Software Bugs: Malware can exploit flaws in software applications or operating systems. For example, a buffer overflow vulnerability	°Data: Malware can steal sensitive information such as personal data, financial records, intellectual property, and trade secrets. Also malware, can encrypt data and demands payment for its release °Networks: Malware can compromise entire networks, leading to data breaches, unauthorized access, and disruption of services °Devices: Malware can infect individual devices like computers, smartphones, tablets, and IoT devices, potentially leading to data loss or device control °Servers: Malware can compromise servers, leading to data breaches, service disruptions, or unauthorized access °Reputation: Malware can lead to reputational damage for organizations, eroding trust and credibility among customers, partners, and stakeholders °Cloud Services: Malware can target cloud environments, affecting data integrity and availability
	Insider	Malicious actors within an organization may create or deploy malware to achieve personal or organizational objectives			
	Hacktivists	Use malware to advance a particular cause, often by disrupting or exposing the activities of individuals or organizations			
Phishing	Cybercriminal	An individual that engages in illegal activities or unethical behavior using computer systems, networks, and	° Stealing Personal Information: attempt to trick individuals into disclosing their usernames, passwords,	° Lack of Awareness: Many individuals are not aware of the tactics and techniques used in phishing attacks, making them more susceptible to falling for fraudulent emails, messages, or websites	° Personal Information: Phishing attacks often aim to steal personal information such as names, addresses, phone numbers, Social Security numbers, and other sensitive data

		digital technologies	credit card information, or other personal and financial data. This information can be used for identity theft, financial fraud, or other malicious purposes ° Credential Theft: target login credentials for various online accounts, such as email, social media, and e-commerce platforms. ° Data breaches: ransomware attacks, or other cybersecurity incidents ° Distributing malicious content, including viruses, ransomware, spyware, and other types of malware ° Fraud: Phishers may impersonate legitimate individuals or organizations to deceive recipients into taking actions that benefit the attacker. This can include sending fake invoices, requesting payments, or redirecting funds to fraudulent accounts	° Human Psychology: Phishing attacks often manipulate human psychology, relying on factors like curiosity, fear, urgency, or empathy to prompt victims to take actions they wouldn't under normal circumstances ° Weak Authentication Processes: If a service or platform has weak authentication processes, attackers may attempt to phish for login credentials to gain unauthorized access ° Lack of Security Awareness Training: Individuals who haven't received proper cybersecurity training are more likely to fall victim to phishing attacks ° Browser Vulnerabilities: Some phishing attacks exploit vulnerabilities in web browsers to display fake content or prompt users to download malicious software	° Email Accounts: Phishing attacks can result in unauthorized access to email accounts, allowing attackers to send malicious emails from the victim's account, distribute spam, or gain access to sensitive information contained in emails ° Financial Information: Attackers may attempt to gather credit card numbers, bank account details, and other financial information to conduct unauthorized transactions ° Network Access: Phishing attacks can provide attackers with access to an organization's internal network, enabling them to infiltrate systems, install malware ° Reputation: Phishing attacks can damage an individual's or organization's reputation if attackers use compromised accounts to spread false information, engage in malicious activities ° Intellectual Property: In business settings, attackers may target intellectual property, trade secrets, research, and development data through phishing attacks ° Employee Accounts: Phishing attacks targeting employees can lead to compromised internal accounts, which can be used for further attacks within an organization
	Nation-State Actors	State-affiliated groups that gather intelligence, conduct espionage, disrupt infrastructure			
	Hacktivists	An individual or group of individuals who employ hacking techniques and digital activism to promote social, political, or ideological causes			
	Insider	Malicious actors within an organization			
	Competitor	Refers to an individual that actively engages in various forms of online activities with the intention of gaining a competitive advantage, causing harm, or achieving specific goals within the digital realm. These activities can include cyber espionage, hacking, data breaches, denial-of-service attacks			
	Scammer	Use various tactics, such as phishing emails, fake websites, social engineering, and other forms of digital manipulation to exploit unsuspecting victims for personal gain, often leading to financial loss or compromising personal data			
	Extremist Groups	Refers to a collection of individuals or entities that employ digital platforms, techniques, and			

		technologies to promote and advance their extremist ideologies, often advocating for radical political, social, or religious beliefs. These groups utilize the internet and various online mediums to spread propaganda, incite violence, engage in hacking activities, and disrupt digital systems, with the intent of furthering their extremist agendas			
DoS	Hacktivists Cybercriminal Competitor Nation-State Actors		° Disruption: The attacker aims to disrupt the availability and accessibility of the target system or service, making it difficult or impossible for legitimate users to access the resources they need ° Resource Exhaustion: DoS attacks often consume critical resources such as bandwidth, processing power, memory, or storage, causing the target system to become slow ° Financial Impact: In some cases, attackers may target online businesses or services, hoping to disrupt their operations and cause financial losses due to downtime or decreased customer trust ° Reputation Damage: Extended downtime or unavailability can lead to a loss of trust among users,	° Application Design Flaws: Poorly designed applications might be vulnerable to attacks that can crash or hang the application, affecting its availability ° Server Misconfiguration: Taking advantage of improperly configured servers or services, which can lead to resource depletion or system instability ° Lack of Redundancy: targeting systems with no redundancy or failover mechanisms can disrupt the service's availability more easily ° not been patched by the vendor or system administrator ° Protocol Vulnerabilities: Exploiting weaknesses in network protocols (e.g., TCP, UDP) or application-layer protocols (e.g., HTTP, DNS) to manipulate or consume resources in an unintended way	° Websites and Online Services: A DoS attack can target websites, making them inaccessible to legitimate users. Online services, such as email servers, cloud platforms ° Network Infrastructure: Routers, switches, and other networking equipment can be overwhelmed by a DoS attack, leading to network congestion and slowdowns ° Servers: Web servers, application servers, and database servers can be overloaded by a DoS attack, causing them to become unresponsive or crash ° Reputation: Organizations can face reputational damage if customers or users cannot access their services, leading to frustration and loss of trust

			customers, partners, and stakeholders ° Competitive Advantage: Attackers might target competitors' systems or services to gain a competitive advantage by disrupting their operations		
Data Breach	Hacktivists Cybercriminal Competitor Nation-State Actors		° Data Theft or Espionage: Attackers may aim to steal sensitive or valuable information, such as personal data, financial records, trade secrets, or intellectual property ° Financial Gain: Some unauthorized access attacks are motivated by financial gains. Attackers may attempt to compromise financial systems, online banking accounts, or payment card information to conduct unauthorized transactions, steal funds ° Disruption: Attackers may target systems with the goal of causing disruption or chaos. This can involve disrupting critical infrastructure, services, or operations, which can lead to financial losses, reputational damage ° Data Manipulation or Destruction: Attackers might seek to alter, manipulate, or delete data within a system, potentially causing data loss,	° Weak Authentication and Access Controls: Many assets come with default usernames and passwords that are often left unchanged, making them an easy target for attackers ° Weak Passwords: Weak, easily guessable, or commonly used passwords are susceptible to brute force attacks ° Lack of Multi-Factor Authentication (MFA): Without MFA, stolen or compromised credentials provide direct access to the asset ° Improper User Privileges: Insufficient segregation of user roles and permissions can allow unauthorized users to gain elevated access ° Unpatched or Outdated Software: Failing to apply security patches and updates leaves assets exposed to known vulnerabilities ° Legacy Systems: Older software or systems may not receive updates, making them susceptible to exploits ° Weak Firewalls and Intrusion Detection Systems: Poorly configured or outdated security appliances can allow unauthorized traffic ° Open Ports and Services: Unused or unnecessary ports and services may provide an entry point for attackers ° Unencrypted Data: Data transmitted or stored without encryption can be intercepted and read by	

			system malfunctions, or creating false information ° System Compromise: Some unauthorized access attacks aim to gain control over systems or networks for malicious purposes. Attackers might create backdoors or establish control over the compromised system, allowing them to launch further attacks ° Cyber Espionage: Nation-states or other groups might engage in unauthorized access attacks to gather intelligence, monitor communications, or infiltrate government or corporate networks for political, military, or economic reasons ° Reputation Damage: Attackers may breach a system to steal sensitive or embarrassing information with the intent of damaging an individual's or an organization's reputation ° Intellectual Property Theft: Unauthorized access attacks can be targeted at stealing valuable intellectual property, including software code, research data, proprietary algorithms, and product designs	unauthorized parties ° Human Exploitation: Attackers can manipulate individuals into divulging sensitive information or granting unauthorized access ° Unauthorized Physical Access: Lack of physical security measures can lead to direct tampering with assets ° Improper Configurations: Incorrectly configured security settings can lead to unintended vulnerabilities ° Inadequate Data Protection: Improper handling of sensitive data can lead to unauthorized access	
Man-in-the-	Hacktivists		° Sensitive Information	° Weak Encryption or No Encryption: If the	° Email: MitM attacks can compromise email

Middle (MitM)	Hacker		Theft: MitM attacks can also target encrypted communications to steal encryption keys or certificates, allowing the attacker to decrypt and access sensitive information ° Bypassing Security Measures: MitM attacks can be used to bypass security mechanisms like two-factor authentication or encryption, allowing the attacker to gain unauthorized access to systems or data ° Credential Theft: MitM attacks can target authentication processes to steal login credentials (e.g., usernames and passwords). Attackers can then use these credentials to access accounts, systems, or networks and carry out further malicious activities ° Session Hijacking: By intercepting and taking control of an ongoing communication session (such as a web session or a user's login session), the attacker can gain unauthorized access to an account or system ° Data Manipulation: The attacker can modify the content of the intercepted communication before passing it along to the intended recipient. This	communication between parties is not encrypted or is encrypted using weak algorithms, attackers can intercept and read the data being transmitted ° Insecure Protocols: Some protocols, like HTTP instead of HTTPS, are susceptible to interception. Attackers can exploit this by intercepting unencrypted traffic and injecting malicious content ° Unauthenticated Connections: Lack of proper authentication mechanisms allows attackers to establish connections with parties involved and pose as legitimate entities ° Unverified Certificates: If a party doesn't verify the authenticity of certificates during SSL/TLS handshakes, attackers can present fake certificates to intercept encrypted ° Router Vulnerabilities: Exploiting vulnerabilities in routers or switches can give attackers control over network traffic	communication, giving attackers access to email contents, attachments, and potentially allowing them to send malicious emails on behalf of the victim ° Web Traffic: Attackers can intercept HTTP, HTTPS, and other web traffic, potentially gaining access to sensitive information such as login credentials, personal data, and financial details ° Network Communications: MitM attacks can target various types of network communication, including Wi-Fi networks, Ethernet connections ° Internet of Things (IoT) Devices: MitM attacks can target IoT devices, allowing attackers to control or manipulate these devices, leading to privacy breaches or disruptions
	insider				
	Cybercriminal				
	Intelligence Agencies	Government agencies may use MitM attacks as part of lawful interception activities to monitor communications for criminal or national security purposes.			
	Nation-State Actors				

			could involve altering transaction details, messages, or instructions to cause confusion, financial losses		
Social Engineering	Hacktivists		° Information Gathering: Attackers may use social engineering techniques to gather sensitive or confidential information, such as usernames, passwords, financial data, or other personal details ° Unauthorized Access: Social engineering attacks can aim to gain unauthorized access to systems, networks, or physical locations by tricking individuals into divulging security credentials ° Data Theft: Social engineering attacks may be aimed at stealing valuable data, trade secrets, intellectual property, or any other form of digital or physical assets ° Fraud and Financial Gain: Social engineering can also be used to perpetrate various types of fraud ° Identity Theft: Some social engineering attacks involve impersonating individuals to steal their identities, which can lead to further financial fraud and privacy violations	° Lack of Awareness: People who are unaware of the potential risks and tactics used in social engineering are more likely to fall victim to such attacks ° Lack of Training: Insufficient training in recognizing social engineering tactics can make employees more susceptible to manipulation ° Poor Password Practices: Individuals using weak passwords, reusing passwords, or sharing them with others can inadvertently provide attackers with access ° Lack of Multi-Factor Authentication (MFA): Without MFA, attackers who obtain a user's password may gain easy access to accounts and systems ° Lack of Security Culture: Organizations without a strong security culture may have employees who are less vigilant about security risks	° Confidential Information: Attackers can manipulate individuals to reveal sensitive information such as passwords, login credentials, personal identification numbers (PINs), and access codes ° Personal Identity: Attackers can steal personal information for identity theft, which may lead to financial loss, fraudulent activities, or reputational damage ° Reputation and Brand Image: Manipulating individuals or employees into disclosing information that could harm a company's reputation or compromise its brand image ° Human Resources: Attackers can target human resources departments to obtain employee information, payroll data, or other sensitive HR-related information ° Operational Processes: Attackers can manipulate employees into altering normal operational processes, potentially leading to disruptions, data breaches, or financial losses ° Healthcare Information: Social engineering attacks can compromise the confidentiality of patients' medical records, leading to privacy breaches and potential misuse of sensitive health data
	Hacker				
	insider				
	Cybercriminal				
	Corporate Espionage	Competing companies or individuals seeking to gain an edge in business may use social engineering to extract proprietary information, trade secrets, or intellectual property from their rivals			
	Challenge Seeker	Some individuals engage in social engineering for the thrill of testing their skills or curiosity about what they can achieve			

			° Espionage: State-sponsored or corporate espionage can involve social engineering to infiltrate organizations, gain insider information, or compromise national security		
Zero-Day Exploit	Criminal Organizations	These groups may engage in activities like hacking into financial systems, stealing personal information, or conducting large-scale cyberattacks	° Unauthorized Access ° Data Theft ° Espionage ° Sabotage ° Financial Gain ° Reputation Damage ° Cyber Warfare	° Software Bugs: Zero-day exploits often target software bugs, such as buffer overflows, memory corruption, race conditions, and input validation errors ° Operating System Vulnerabilities: Zero-day exploits can target vulnerabilities in operating systems, such as privilege escalation flaws, kernel-level vulnerabilities ° Vulnerabilities in network services, such as remote desktop protocols, web servers, and email servers, can be exploited to gain unauthorized access or execute arbitrary code on the target system ° weaknesses in authentication and authorization mechanisms, allowing attackers to bypass security measures and gain unauthorized access ° convincing users to perform actions that inadvertently expose vulnerabilities. For example, a user might be tricked into clicking a malicious link or opening a malicious attachment ° Vulnerabilities in server software, such as web servers (e.g., Apache, Nginx), database servers (e.g., MySQL, PostgreSQL), and application servers	° Network Infrastructure: Routers, switches, firewalls, and other network infrastructure components may be targeted to gain control over a network or to intercept and manipulate traffic ° Applications: Any software applications that are commonly used, such as office suites, media players, communication tools, and more, could be targeted via zero-day exploits ° Embedded Systems: Embedded systems found in various devices, such as medical equipment, automotive systems, and industrial control systems, can also be targeted ° Virtualization Software: Hypervisors and virtualization platforms are potential targets ° Cloud Services: Vulnerabilities in cloud service platforms and providers can lead to unauthorized access to sensitive data stored in the cloud
	Security Researchers	may discover and use zero-day exploits for legitimate purposes, such as identifying vulnerabilities, testing and improving security measures, and helping organizations enhance their defenses			
	Nation-States	Some countries and government agencies may develop or purchase zero-day exploits as part of their cyber espionage or cyber warfare efforts			
	Cybercriminals	These are individuals or groups with malicious intent who seek to exploit zero-day vulnerabilities for financial gain, data theft, disruption of services, or other malicious activities			
Theft of Hardware	Criminals and Opportunistic Thieves	These are individuals who engage in theft for personal gain. They might steal IT hardware such as laptops,	° Monetary Gain: Stolen IT hardware, such as laptops, servers, and networking equipment, can be sold on	° Lack of Physical Security: Insufficient physical security measures, such as unlocked doors, unmonitored access points, or lack of surveillance cameras, can make it easier for thieves to gain	° Physical Hardware: Stolen IT hardware includes items such as laptops, desktop computers, servers, routers, switches, and other network equipment

		smartphones, and servers to sell on the black market	the black market for a profit ° Data Breaches: Thieves might steal IT hardware to gain access to sensitive data stored on the devices ° Resale or Use: Some thieves may steal IT hardware for personal use or to sell to unsuspecting individuals ° Sabotage: Theft of IT hardware can disrupt the operations of a business, organization, or individual. By stealing critical hardware components like servers or networking equipment, thieves can cause significant downtime and financial losses	access to IT hardware ° Unattended Equipment: Leaving IT hardware unattended, especially in public spaces or unsecured areas, creates an opportunity for theft ° Inadequate Employee Training: Lack of training and awareness among employees about security risks and protocols can lead to carelessness and inadvertent theft ° Untracked Inventory: Poor inventory management and tracking can make it difficult to detect missing hardware until it's too late ° Inadequate Monitoring: Lack of real-time monitoring for unusual activities or unauthorized access can delay the detection of theft ° Unsecured Storage: Leaving laptops, tablets, or other portable devices in vehicles or unsecured storage areas can make them easy targets for theft ° Disposal of Equipment: Insecure disposal practices can lead to theft if hardware containing sensitive data is not properly wiped or destroyed ° Unsecured Peripherals: Peripherals such as external hard drives, USB drives, and printers can be stolen if left unsecured ° Lack of Deterrents: Visible deterrents such as security cameras, locks, and signage can discourage potential thieves	° Data and Information: Stolen hardware might contain sensitive or confidential data, such as customer information, financial records, intellectual property, trade secrets, and proprietary software ° Network Infrastructure: Theft of network equipment can disrupt an organization's network infrastructure, affecting connectivity, communication, and data flow ° Reputation: If stolen hardware contains sensitive or personal information, a data breach could lead to a loss of trust among customers, partners, and stakeholders. This damage to the organization's reputation can have far-reaching consequences
	Insiders	Employees or contractors within an organization may steal IT hardware due to disgruntlement, financial incentives, or other personal reasons			
	Hacktivists				
	Competitors				
	Terrorist Groups	terrorist organizations might steal IT hardware to support their activities or gather information for planning attacks			
Destruction of equipment	Malicious Hackers	Cybercriminals and hackers may intentionally destroy IT equipment as part of a cyberattack	° Sabotage and Disruption: Attackers may seek to disrupt the operations of an organization ° Revenge or Retaliation: Individuals or groups with grievances against an organization may resort to destroying IT equipment as	° Uncontrolled Access: Unauthorized access to IT equipment can result in intentional or accidental damage, theft, or tampering ° Environmental Factors: Poor environmental conditions, such as extreme temperatures, humidity, dust, or inadequate cooling, can lead to overheating or corrosion of IT equipment components ° Insufficient Maintenance: Lack of regular	° Data and Information: IT equipment often stores critical data and information ° Hardware Assets: The IT equipment itself, including servers, computers, networking devices, and peripherals, is a valuable asset ° Software Assets: IT equipment may host software applications and licenses
	Insiders	Employees, contractors, or individuals with authorized access to IT systems may cause equipment destruction due to various reasons,			

		including revenge, sabotage, or personal motivations	a form of retaliation. This could be due to personal conflicts, legal disputes, or other disagreements ° Competitive Advantage: In some cases, attackers may aim to gain a competitive advantage by crippling the IT infrastructure of a rival organization ° Ideological Reasons: Certain attackers, such as hacktivists or cyberterrorists, may engage in destructive actions to promote a particular ideology	maintenance, cleaning, and updates can lead to the gradual deterioration and eventual failure of IT equipment	° Network Assets: Networking equipment, such as routers, switches, and firewalls, are essential for communication and data transfer within an organization ° Operational Assets: Many businesses rely on IT equipment to carry out daily operations. Destruction of IT equipment can disrupt business processes ° Reputation and Brand Assets: IT disruptions caused by the destruction of equipment can lead to negative customer experiences, loss of trust
	Terrorists	terrorist groups may target IT infrastructure to disrupt critical services, communication networks, or government operations			
	Vandalism	Random acts of vandalism or mischief can also lead to the destruction of IT equipment, particularly in unsecured locations			
SQL injection	Hackers Hacktivists Competitors Insiders State-Sponsored Actors		° Unauthorized Data Access: Attackers may use SQL injection to bypass authentication and gain unauthorized access to sensitive data stored in a database ° Data Exfiltration: Once attackers gain access to the database, they can extract data from it and steal sensitive information. This stolen data can then be used for identity theft, financial fraud, or other malicious purposes ° Data Manipulation: SQL injection can allow attackers to alter, delete, or modify data within the database	° Lack of Input Validation: When an application does not properly validate user inputs, attackers can inject malicious SQL code into input fields, leading to unauthorized access to the database ° Error Messages Disclosure: If error messages from the database are displayed directly to users, attackers can exploit these messages to gain insights into the database structure and use that information to craft malicious SQL queries ° Inadequate Authentication and Authorization: SQL injection attacks can also exploit weaknesses in authentication and authorization mechanisms, allowing attackers to access or modify data they shouldn't have access to	° Application and Server Compromise: In severe cases, attackers may be able to exploit SQL injection vulnerabilities to take control of the application or underlying server, potentially leading to a complete system compromise ° Sensitive Operations: SQL injection can be used to perform operations that can lead to financial loss, such as transferring funds, altering transaction records ° Data: An attacker can gain unauthorized access to sensitive data stored in a database, including personal information, financial records, passwords, and other confidential data, Attackers can modify or delete data stored in the database. SQL injection attacks can lead to denial-of-service (DoS) scenarios by overwhelming the database server with malicious queries, causing it to become unresponsive or crash

			° Privilege Escalation: By exploiting SQL injection vulnerabilities, attackers may be able to escalate their privileges within the database system. This could enable them to perform actions they wouldn't normally have permission to do, such as creating new users, modifying access controls ° Denial of Service (DoS): In some cases, attackers may use SQL injection to execute malicious queries that cause the database or application to become unresponsive or crash ° Application Defacement: SQL injection attacks might also be used to modify the content displayed by a web application. Attackers could inject malicious scripts or content into a website, potentially defacing it ° Malware Injection: In more sophisticated attacks, attackers might inject malware or malicious code into the database, which could then be executed within the context of the database server ° Lateral Movement: If the database server is part of a larger network or environment, attackers could		

			potentially use a successful SQL injection attack as a stepping stone to pivot within the network and move laterally to other systems ° Reputation Damage: Successful SQL injection attacks can lead to significant reputational damage for organizations		
Brute Force	Hackers		° Password Cracking: Brute force attacks are commonly used to crack passwords ° Account Takeover: Attackers may use brute force attacks to gain control over user accounts on various platforms, such as email accounts ° Network Access: Brute force attacks can target network devices, routers, and firewalls in an attempt to gain unauthorized access to a corporate network ° Software Cracking: Brute force attacks can also be used to crack software license keys or activation codes	° Weak passwords: If a system has users with weak passwords, such as common words, easily guessable patterns, or short lengths, it becomes vulnerable to Brute Force Attacks ° Lack of account lockout or rate limiting: Without mechanisms in place to prevent multiple failed login attempts within a short period of time, attackers can keep trying different passwords until they find the correct one ° Insufficient password complexity requirements: Systems that do not enforce strong password policies, including requirements for a mix of characters (uppercase, lowercase, numbers, symbols) and a minimum length, are more susceptible to Brute Force Attacks ° Insufficient password complexity requirements: Systems that do not enforce strong password policies, including requirements for a mix of characters (uppercase, lowercase, numbers, symbols) and a minimum length, are more susceptible to Brute Force Attacks	° Network Services: Network services like Remote Desktop Protocol (RDP), SSH, and FTP can be compromised if weak passwords are used ° Network Services: Network services like Remote Desktop Protocol (RDP), SSH, and FTP can be compromised if weak passwords are used ° Data: Brute force attacks can be used to attempt to gain access to confidential information
	Criminal Organizations				
	State-Sponsored Actors				
	Hacktivists				
	Insiders				
	Script Kiddies	Inexperienced individuals who use pre-made hacking tools or scripts to engage in attacks, including brute force attacks, without a deep understanding of the underlying mechanisms			

				° Lack of multi-factor authentication (MFA): Systems without MFA are more vulnerable to Brute Force Attacks because even if an attacker guesses the password, they would still need the second factor to gain access	
USB-Based Threats	Cybercriminals Hacktivists Hackers insiders		° Data Theft: Attackers may use USB threats to steal sensitive data, such as personal information, financial details, intellectual property, or trade secrets ° Malware Propagation: USB devices can serve as a vector for spreading malware, such as viruses, worms, Trojans, and ransomware, from one system to another ° Espionage: In targeted attacks, USB threats can be used for corporate or government espionage. Attackers may physically insert USB devices into a target organization's network to gather sensitive information ° Destruction or Disruption: Some USB threats aim to disrupt computer systems or networks	° Autorun and AutoPlay Exploitation: USB devices can take advantage of autorun and AutoPlay features to automatically execute malicious code when connected to a computer ° Lack of Device Authentication: Some systems do not properly authenticate USB devices, allowing attackers to plug in rogue devices that can then execute malicious commands ° Outdated Software: If a system's operating system or software has known vulnerabilities, connecting a malicious USB device could trigger an exploit against those vulnerabilities	° Computers and Laptops: USB threats can target the operating system, applications, and data stored on computers and laptops ° Servers: USB attacks can impact servers in data centers or local networks, potentially causing data breaches ° Networks: USB threats can be used to spread malware across networks, enabling attackers to gain control over networked devices, infiltrate systems ° Sensitive Information: USB threats can target sensitive data, including personal information, financial data, intellectual property, and other confidential information

DNS poisoning			° Data Exfiltration: DNS can be used as a covert channel for sending sensitive data out of a compromised network. Attackers can encode data into DNS queries or responses and send them to a controlled server outside the network, bypassing traditional security controls ° Disruption of Services: By poisoning DNS records, attackers can cause legitimate users to be unable to access specific websites or online services ° Espionage and Surveillance: DNS poisoning can be used for surveillance purposes, redirecting specific users or organizations to malicious servers that log their activities or capture sensitive information	° Lack of Source Authentication: DNS was originally designed without strong authentication mechanisms, making it susceptible to attackers who can impersonate legitimate DNS servers and send false DNS responses ° Cache Pollution: DNS caching servers often do not perform proper validation of received DNS responses, making them susceptible to accepting and storing malicious or forged responses ° Insufficient DNSSEC Implementation: DNS Security Extensions (DNSSEC) help protect against DNS poisoning by digitally signing DNS records ° Slow Cache Expiration: Longer cache expiration times can increase the potential impact of DNS poisoning attacks	° Websites: Legitimate websites can be redirected to malicious sites, leading to potential data theft, phishing, or malware distribution ° Email Services: DNS poisoning can redirect email traffic, leading to interception of sensitive emails or distribution of spam ° Network Resources: DNS poisoning can disrupt access to internal network resources, affecting business operations and communication ° DNS Servers: The DNS servers themselves can be compromised, leading to further propagation of malicious DNS information
Fake Software	Malware creators		° Malicious Intent: gain unauthorized access to a user's system, steal sensitive information	° Lack of User Awareness: Many users are not well-informed about the risks associated with downloading and installing software from untrusted sources	° Computers and Devices: Fake software can infect computers, smartphones, tablets, and other devices ° Data and Information: Malicious software can steal,

					corrupt, or delete valuable data, including personal files, financial records, passwords, and more
			° Financial Gain: Cybercriminals often distribute fake software as a means to generate revenue. They may use tactics like scareware, where a fake software claims to have detected threats on the user's system and demands payment for their removal ° Phishing: Fake software can also be used as a part of phishing campaigns. Cybercriminals may create fake software updates or applications that mimic legitimate ones to trick users into downloading and installing them. These fake programs can then be used to gather sensitive information ° Espionage: Nation-states and other entities may develop and deploy fake software to conduct espionage activities ° Sabotage: In some cases, fake software may be installed to disrupt the normal functioning of a system or organization	° Outdated Software and Security Patches: Running outdated software and failing to apply security patches can leave systems vulnerable to exploitation. Attackers may take advantage of known vulnerabilities in outdated software to install fake software ° Weak Passwords and Credentials: Poor password practices can lead to unauthorized access to accounts and systems. Cybercriminals who gain access to a user's account can manipulate software downloads and install fake applications	° Networks and Infrastructure: Fake software can compromise network security, leading to potential breaches of entire systems, servers, and databases ° Operational Disruption: Organizations may face operational disruptions due to fake software, leading to downtime, data loss, and potential financial losses

4.4. Impact

The term "impact" refers to the potential consequences or effects of a threat event on an organization's assets. It can be:

Financial Impact: The potential monetary losses due to a threat event

Reputation Impact: The damage or harm that could be inflicted upon an organization's reputation, credibility, and public perception

Legal Impact: The legal consequences, liabilities, and legal actions that an organization might face due to a threat event

Operational Impact: The disruptions that may occur within an organization's day-to-day operations as a result of a threat event

Business Continuity Impact: The interruption to an organization's ability to continue its business functions

Example:

Scenario	Impact
A ransomware attack (feared event) compromises sensitive data (business asset) resulting in reputational damage	Reputational damage
Malware infection spreading across internal network (feared event) impacts confidential documents (business asset)	Sensitive Data disclosure
Theft of company laptops (feared event) lead to disclosure of sensitive data (business asset) stored on them	Sensitive data disclosure
A data breach (feared event) exposes credit card information (business asset)	Data breach
Malicious modification (feared event) alters critical files (business asset)	Illegal modification
Business Continuity Impact: The interruption to an organization's ability to continue its business functions	Process disruption
An external hacktivist group successfully defaced the company website temporarily	Web defacement
A minor malware infection affected a non-critical system due to a user's inadvertent download of a malicious file, causing only isolated disruption and minimal data loss	Disruption

4.5. Information Security Risk

Risk is the likelihood of a threat exploiting a vulnerability, resulting in a negative impact on an organization's operations, assets, or objectives. Risk is the likelihood that a loss will occur. Some risks are so severe, Other risks are minor and can be accepted. We must differentiate severe risks from minor risks, when this is done properly, administrators and managers can intelligently decide what to do about any type of risk. The end result is one option of:

- Avoid the risk
- Transfer the risk
- Mitigate the risk
- Accept the risk

Company that ignores risk can fail. Risk can be mitigated by reducing vulnerabilities or reducing the impact.

The concept of risk in the context of risk management is often represented as the product of likelihood and impact. This approach helps quantify and prioritize risks by considering both the probability of an event occurring (likelihood) and the potential consequences if it does occur (impact). The formula for calculating risk is:

Risk = Likelihood × Impact

For example, if we have a risk event with a high likelihood (70% chance) and a high impact (potential financial loss of $1 million), the calculated risk would be:

Risk = 0.70 (likelihood) × $1,000,000 (impact) = $700,000

Or

For example, if we have a risk event with a high likelihood (4) and a high impact (3), the calculated risk would be:

Risk = 4 (likelihood) × 3 (impact) = 12

The following sentences develop some Risk scenarios identification:

High Impact Scenarios :

Risk 1: A phishing threat, initiated through a deceptive email containing a malicious link, exploited the vulnerability of human susceptibility to social engineering, leading to the compromise of employee workstations and sensitive data. This compromise could lead to identity theft, and potential financial losses.

Risk 2: The infiltration of ransomware into the server infrastructure stemmed from a compromised software update, exploiting an unpatched vulnerability, and resulting in the encryption of critical business data. This infiltration led to financial losses and damages the organization's reputation.

Risk 3: The compromise of the customer database due to lack of access control, could result in loss of customer trust, legal consequences and financial penalties.

Risk 4: The disruptive impact on the web server and online services due to a DDoS attack could lead to loss of revenue, damage to the organization's online presence, and customer dissatisfaction.

Risk 5: Unauthorized access to sensitive cloud storage could lead to exposure of confidential documents, potential legal consequences, and damage to the organization's reputation.

Risk 6: Unauthorized manipulation of financial transactions and data could lead to financial losses, regulatory fines, and legal liabilities for the organization.

Risk 7: The exposure of customer payment information through an SQL injection attack could result in financial fraud, identity theft, and loss of customer trust.

Risk 8: The compromise of a user's computer and personal data due to a zero-day exploit could result in data theft, unauthorized access to accounts, and potential financial losses.

Risk 9: The divulgence of user credentials and sensitive information through a social engineering attack could lead to unauthorized access, data breaches, and potential financial losses for individuals and the organization.

Medium Impact Scenarios :

Risk 10: An external hacktivist group successfully defaced the company website temporarily, leading to a moderate loss of credibility and necessitating rapid restoration efforts to mitigate potential brand damage.

Low Impact Scenarios :

Risk 11: A minor malware infection affected a non-critical system due to a user's inadvertent download of a malicious file, causing only isolated disruption and minimal data loss.

Risk 12: A Temporary service interruption occurred as a result of a misconfiguration error in network equipment settings, causing brief disruption but with negligible financial impact.

Risk 13: Unauthorized access to publicly available information took place due to misconfigured cloud storage with public access, leading to limited data exposure and no compromise of sensitive information.

The following table provides information for the previously listed IT risk scenarios:

Risk	Threat	Actor	Exploited vulnerability	Impact	Impact Severity
Phishing Attack on Employee Workstations	Phishing	Hacker	Lack of awareness	Data breaches, identity theft, potential financial loss	High
Ransomware Targeting Server	Ransomware	External attacker	Unpatched software vulnerability	Disrupted operations, financial loss, reputation damage	High
DDoS Attack on Web Server	DDoS Attack	Cyber terrorist	Lack of adequate network traffic filtering	Revenue loss, online presence damage, customer dissatisfaction	High
Malware Infection Through Unpatched Software	Malware	Insider	Unpatched software vulnerability	Identity theft, unauthorized account access, data loss	High
Unauthorized Access to Cloud Storage	Unauthorized access	Malicious actor	Insecure authentication methods	Confidential data exposure, legal consequences	High
Insider Attack on Financial Transactions	Insider attack	Insider	Insufficient role-based access controls	Financial losses, regulatory fines, legal liabilities	High
SQL Injection Attack on E-Commerce Database	SQL injection	External attacker	Lack of input validation and sanitization	Financial fraud, identity theft, loss of customer trust	High
Zero-Day Exploit in Web Browser	Zero-day exploit	Hacker	Unknown vulnerability in the web browser	Data theft, unauthorized access, potential financial loss	High
.....	.....	.....	.....	.....	.....

In the IT Infrastructure, we can examine risks in the following domains:

User:

Phishing and Social Engineering: Users may fall victim to phishing emails or social engineering tactics, leading to unauthorized access to sensitive data or system compromise.

Weak Passwords: Users using weak passwords or reusing passwords across multiple accounts can lead to unauthorized access and data breaches.

Insider Threats: Malicious actions or unintentional mistakes by employees with access to sensitive information can result in data leaks or security breaches.

Lack of Security Awareness: Users not being educated about security best practices could inadvertently engage in risky behavior, such as clicking on malicious links or downloading infected files.

Workstation:

Malware and Viruses: Workstations can become infected with malware or viruses, potentially leading to data loss, unauthorized access, or system disruption.

Unpatched Software: Failure to apply security patches and updates can leave workstations vulnerable to known vulnerabilities.

Data Leakage: Improper data handling practices on workstations can lead to accidental data leakage or breaches.

Unauthorized Access: Weak access controls can result in unauthorized users gaining access to workstations and sensitive information.

Network:

Data Interception: Weak network security can allow attackers to intercept and eavesdrop on data transmissions.

Denial of Service (DoS) Attacks: Networks can be targeted with DoS attacks, causing service disruptions and downtime.

Unauthorized Access: Insufficient network access controls can lead to unauthorized users gaining access to network resources.

Network Segmentation Issues: Poorly segmented networks may allow attackers to move laterally within the network, increasing the scope of a breach.

Application:

Code Vulnerabilities: Flaws in application code can be exploited by attackers to gain unauthorized access or execute malicious actions.

SQL Injection: Poorly sanitized inputs can lead to SQL injection attacks, allowing attackers to manipulate databases.

Unvalidated Inputs: Lack of input validation can lead to data integrity issues and potentially allow attackers to insert malicious data.

Inadequate Authentication: Weak authentication mechanisms can lead to unauthorized access to applications and data.

5. Security Controls

Information security controls are the safeguards that an organization implements to protect its sensitive information from unauthorized access, disclosure, alteration, or destruction. These controls are a critical component of an organization's overall information security program and are designed to mitigate various risks that could compromise the confidentiality, integrity, and availability of information systems.

Classification par type

Information security controls can be broadly categorized into four main types:

a. **Administrative Controls**: These controls encompass policies, procedures, guidelines, and standards that define the rules and responsibilities for managing and protecting information. Examples include security policies, security awareness training, access control policies, and incident response plans.

b. **Technical Controls**: These controls involve the use of technology to safeguard information. Examples include firewalls, encryption, intrusion detection systems, antivirus software, and access control mechanisms.

c. **Physical Controls**: These control are designed to protect the physical infrastructure of an organization, such as data centers and offices. Examples include biometric access control systems, surveillance cameras, locks, and environmental controls like fire suppression systems.

D. **Legal Controls**: related to the application of a ligeslation, regulatory requirements and contractual obligation, These controls are crucial for organizations that handle personal data, financial information, intellectual property, and other sensitive data. (ex : regulations like HIPAA in the U.S)

Classification par fonction

a. **Detective Control:** are designed to identify and detect security incidents or unauthorized activities after they have occurred. Their primary purpose is to provide visibility into potentially malicious or unauthorized actions or incidents (ex : SIEM, IDS/IPS, log, camera).
b. **Preventive Control :** are implemented to proactively reduce the likelihood of security incidents or unauthorized access. They aim to prevent security threats from materializing (ex : Firewalls, Security awareness training, Security policies and procedures)
c. **Corrective control** : are put in place to remediate or mitigate the impact of a security incident or breach after it has been detected. These controls help to recover from security events and prevent similar incidents in the future (ex : Incident response plans, Backup and disaster recovery, Patch management to fix vulnerabilities)

Exercice 4:

Organization Context:

XYZ Financial Services is a mid-sized financial institution that provides a wide range of financial products and services, including banking, investment, and insurance. They have a large customer base, handle sensitive financial data, and are subject to various financial industry regulations. XYZ Financial Services is committed to maintaining the confidentiality, integrity, and availability of their customers' financial information.

Task: In the context of XYZ Financial Services, identify and classify different information security controls into the following categories: technical, physical, and administrative controls. Additionally, specify whether each control falls into the preventive, detective, or corrective control category.

Solution :

Technical Controls:

1. **Preventive (Technical)**:
    - Two-Factor Authentication: XYZ Financial Services uses two-factor authentication for customer online banking access to prevent unauthorized account access.
2. **Detective (Technical)**:
    - Security Information and Event Management (SIEM) System: A SIEM system is employed to monitor logs, network traffic, and system events for signs of security incidents or unusual activities.
3. **Corrective (Technical)**:
    - Automated Patch Management: An automated system is in place to apply security patches and updates promptly to mitigate vulnerabilities in the organization's software and systems.

Physical Controls:

4. **Preventive (Physical)**:
    - Biometric Access Control: The data center that houses financial data is secured with biometric access controls, limiting physical access to authorized personnel.
5. **Detective (Physical)**:
    - Video Surveillance: Security cameras are installed at the entrances and within the data center to monitor and record physical access.
6. **Corrective (Physical)**:
    - Alarm System: In case of unauthorized access to restricted areas, an alarm system triggers alerts and prompts a security response.

Administrative Controls:

7. **Preventive (Administrative)**:
    - Security Policies and Procedures: XYZ Financial Services has comprehensive security policies and procedures in place, including data handling guidelines and password policies, to guide employees on security best practices.
8. **Detective (Administrative)**:
    - Security Awareness Training: Regular training programs are conducted to educate employees about the latest security threats and how to recognize and report suspicious activities.
9. **Corrective (Administrative)**:
    - Incident Response Plan: The organization maintains an incident response plan, outlining the steps to follow in case of a security incident, including containment, eradication, and recovery procedures.

6. Definition of the ISMS

An Information Security Management System (ISMS) is a structured and comprehensive approach to managing and protecting an organization's sensitive information. It is designed to systematically identify, assess, manage, and reduce information security risks, ensuring the confidentiality, integrity, and availability of information assets.

Key Components of an ISMS:

1. **Policies and Procedures**: An ISMS begins with the development of policies and procedures that outline the organization's approach to information security. These documents set the foundation for how information will be protected and define roles and responsibilities.
2. **Risk Assessment**: A critical aspect of an ISMS is the identification and assessment of information security risks. This involves identifying potential threats and vulnerabilities and evaluating the potential impact of security incidents.
3. **Risk Management**: After assessing risks, an ISMS focuses on risk management strategies. This includes developing and implementing controls, safeguards, and countermeasures to mitigate or accept identified risks.
4. **Security Awareness and Training**: ISMS includes provisions for educating employees and stakeholders about security policies, best practices, and potential risks. Security awareness and training help create a security-conscious culture.
5. **Incident Response Plan**: An effective ISMS has an incident response plan in place to address security incidents promptly and effectively. This plan outlines procedures for reporting, containing, investigating, and mitigating security breaches.
6. **Continuous Improvement**: An ISMS follows a cycle of continuous improvement. It regularly reviews and revises policies, assesses new risks, and adapts to changing security threats and regulatory requirements.
7. **Compliance and Audit**: ISMS includes mechanisms for compliance monitoring and auditing to ensure that the organization is meeting its security objectives and adhering to relevant standards and regulations.
8. **Documented Information**: Maintaining and managing documented information, such as security policies, risk assessments, and incident reports, is a crucial part of an ISMS.

Standards and Frameworks: ISMS implementations often align with internationally recognized standards, such as ISO/IEC 27001, which provides a systematic approach to information security management. Additionally, frameworks like NIST Cybersecurity Framework.

Benefits of an ISMS:

1. **Enhanced Security**: An ISMS helps organizations identify and mitigate security risks effectively, reducing the likelihood of security incidents.
2. **Compliance**: It facilitates compliance with industry regulations, legal requirements, and contractual obligations.
3. **Data Protection**: It ensures the protection of sensitive data, which is essential for maintaining the trust of customers and stakeholders.
4. **Business Continuity**: A robust ISMS aids in maintaining business continuity by minimizing the impact of security incidents.
5. **Improved Reputation**: Effective information security management enhances an organization's reputation and trustworthiness.
6. **Cost Savings**: By proactively addressing security risks, organizations can save money by avoiding costly security breaches.
7. **Competitive Advantage**: Demonstrating a strong commitment to information security can provide a competitive advantage in the marketplace.

Exercice 5: Implementing ISMS

Scenario: You are the owner of a small e-commerce business that sells handmade crafts. You have heard about the importance of information security and want to establish an ISMS to protect your customer data and business information.

Task: Design an ISMS for your small business. Consider the following aspects:

1. **Risk Assessment**:
    - Identify potential information security risks specific to your business, such as data breaches, website attacks, or insider threats.
2. **Risk Management**:
    - Determine how you will mitigate the identified risks. For example, you might decide to encrypt customer data, implement a firewall, or provide security training for your employees.
3. **Access Control**:
    - Define who should have access to sensitive data, like customer records and payment information. How will you control access to this data?
4. **Incident Response Plan**:
    - Develop a simple incident response plan. What will you do if there's a data breach or a cyberattack? Who should be notified, and what steps will you take to contain the incident?
5. **Security Awareness**:
    - Consider how you will educate your employees about security best practices. This could be through training sessions or informative materials.
6. **Documentation**:
    - Create a basic set of security policies and procedures. Include how data should be handled, password policies, and what to do in case of a security incident.

Solution:

1. **Risk Assessment**:
    - Identify Risks: You identify potential risks like customer data exposure, online payment fraud, and website defacement.
2. **Risk Management**:
    - Mitigation: To mitigate these risks, you decide to encrypt customer data using SSL certificates for your website. You also install a firewall to protect against unauthorized access.
3. **Access Control**:
    - Access List: You maintain a list of authorized employees who can access customer payment information. You implement strong password policies to secure access.
4. **Incident Response Plan**:
    - Incident Reporting: You establish a process to report security incidents to you. In case of a data breach, you will inform affected customers, contact authorities if necessary, and take steps to prevent future breaches.
5. **Security Awareness**:
    - Training: You schedule security training sessions for your employees to teach them about the importance of security, recognizing phishing attempts, and safe internet practices.
6. **Documentation**:
    - Policies and Procedures: You create a set of documents, including a data handling policy, password policy, and an incident response procedure.

Exercise 6: Benefit of the ISMS

Scenario: You work as an IT manager for a medium-sized company, and you are considering implementing an ISMS. To understand the potential benefits, you decide to evaluate the situation before and after the implementation of an ISMS.

Task: Identify and describe the potential benefits of implementing an ISMS in the scenario below.

Scenario: **Before ISMS Implementation**:

Your company is experiencing the following challenges:

- Frequent data breaches resulting in loss of customer data and damage to the company's reputation.
- Disorganized and inconsistent information security practices.
- Difficulty in maintaining compliance with industry regulations and legal requirements.
- Lack of a clear incident response plan, leading to inefficiency in handling security incidents.
- Increased financial losses due to security incidents and subsequent legal actions.

After ISMS Implementation:

You've successfully implemented an ISMS, which includes policies, procedures, and controls for information security.

Benefits:

- **Reduced Data Breaches**: Data breaches have significantly reduced due to the implementation of security controls. This has helped maintain customer trust and avoid legal repercussions.
- **Standardized Practices**: Information security practices are now consistent and well-documented, making it easier for employees to follow best practices.
- **Regulatory Compliance**: The ISMS has ensured that the company complies with industry regulations and legal requirements, preventing fines and penalties.
- **Efficient Incident Response**: With a clear incident response plan, security incidents are now handled efficiently, reducing potential damage and recovery time.
- **Financial Savings**: The company has experienced financial savings by avoiding data breach costs, legal actions, and regulatory fines.

Solution:

The scenario above illustrates several key benefits of implementing an ISMS:

1. **Risk Reduction**: The ISMS has reduced the risk of data breaches, leading to a more secure environment and lower costs associated with breaches.
2. **Consistency**: The ISMS has standardized information security practices, making it easier for employees to understand and follow security procedures.
3. **Compliance**: Compliance with industry regulations and legal requirements is achieved, reducing the risk of penalties and fines.
4. **Efficiency**: The efficient handling of security incidents minimizes potential damage and recovery time, saving both time and money.
5. **Cost Savings**: Overall, the ISMS has resulted in significant cost savings by avoiding data breach expenses, legal actions, and regulatory fines.

4 - Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

- Understand the environment in which the organization seeks to achieve its objective.

- This clause refers to the understanding that an organization must have about its internal and external environment.

- Determine and analyze the external and internal issues.

External Issues:

External issues are factors outside the organization that can influence its information security objective.

The (**PESTLE**) model is a strategic framework used to analyze and evaluate the external environmental factors that can impact an organization's information system.

1. **Political**:
    - *Definition*: Political factors refer to the influence of government policies, regulations, and political stability on an organization. This includes factors like government stability, and regulatory changes.
    - Political instability can increase security risks. During protests or upheaval, there is a higher likelihood of cyberattacks, data breaches, and unauthorized access to sensitive information. **Information systems must be fortified to withstand increased security threats.**

2. **Environmental**:
    - *Definition*: Environmental factors encompass the influence of ecological and environmental conditions on an organization. This includes sustainability, climate change, natural disasters, and environmental regulations.
    - Natural disasters like earthquakes, floods, or hurricanes are external environmental issues that can disrupt an organization's information systems. **Organizations need to consider the physical location and disaster recovery plans for their data centers to ensure system availability during such events.**

3. **Social**:
    - *Definition*: Social factors involve the influence of societal and cultural aspects on an organization. This includes demographics, consumer behavior, cultural norms, social trends, and values.
    - The high crime rate in the area can lead to security concerns for the organization's information systems. There may be an increased risk of physical theft, vandalism. **The organization may need to invest in enhanced physical security measures to protect its data centers and IT infrastructure. This can include secure access controls, surveillance systems, and alarms to prevent unauthorized access and protect sensitive equipment.**

4. **Technological**:
    - *Definition*: Technological factors refer to the impact of technological advancements and innovation on an organization. This includes technology infrastructure, research and development, automation, and digital trends.
    - a technological factor such as poor telecommunication infrastructure in a country can significantly affect an organization's information system. Poor telecommunication infrastructure can lead to frequent connectivity issues, including slow internet speeds, dropped connections, and network instability. This can result in delays and interruptions in data transmission, affecting the availability and performance of information systems. **Implementing load balancing to distribute network traffic across multiple servers or network paths can help to ensure a more even distribution of data traffic and reduce the impact of poor connections.**

5. **Legal**:
    - *Definition*: Legal factors involve the impact of laws and regulations on an organization. This includes labor laws, data protection regulations, intellectual property rights, and industry-specific regulations.
    - Legal factors can influence information systems through regulatory compliance requirements. For instance, data protection laws like the GDPR (General Data Protection Regulation) mandate strict data privacy and security standards. **Organizations must adapt their information systems to comply with these regulations, which can involve implementing encryption, access controls, and data retention policies.**

6. **Economic**:
    - *Definition*: Economic factors encompass the influence of economic conditions on an organization. This includes factors like inflation, exchange rates, economic growth, and consumer spending.
    - In a competitive landscape, economic issues can motivate organizations to engage in corporate espionage. This can lead to attempts to breach competitors' information systems to gain a competitive advantage or steal sensitive information. **A strong cybersecurity posture and threat detection capabilities are crucial to defend against such threats.**

Internal Issues:

- Internal issues are factors and conditions within the organization that can impact its information security management. This could involve :

1. Information system : example the lack of control over the installation of new systems that will replace the old ones, can introduce risks to an organization's information systems, such as compatibility issues, security vulnerabilities, and operational disruptions. **Organization must provide training and awareness programs for employees involved in system installations. They should understand the importance of following procedures and best practices to mitigate risks.**

2. Organization culture : exemple a historical failure to respect confidentiality needs by employees can significantly impact an organization's culture and information security. This issue can manifest in various ways, affecting the organization's work environment, trust, and overall security posture. **Addressing this issue requires a cultural shift within the organization. Leadership must emphasize the importance of confidentiality, set an example, and promote a culture of trust and responsibility.**

3. Limited staff skills : Inadequate skills can lead to inefficient operation of information systems. Staff may struggle to troubleshoot and resolve technical issues promptly, resulting in downtime and productivity losses. **Organization can provide ongoing training and development opportunities for staff to enhance their technical skills. This could include courses, workshops, certifications, and access to relevant resources.**

4. Role and responsabilities : example responsabilities are retained by a small team. A small team may lack the diversity of skills and expertise needed to address all aspects of information system management effectively. Knowledge can become concentrated in a few individuals, making the organization vulnerable if team members leave or are unavailable. **Organization can develop a clear plan for how the information system team will scale as the organization grows. This might involve hiring additional staff or working with external partners.**

Evaluation of 4.1:

1) Have you determined the external and internal issues specific to the purpose of your organization and affecting your ability to achieve the expected results of your information security management system ?

How to do :

Table for Determining External and Internal Issues Impacting ISMS:

Issues	Description	Relevance to ISMS	Impact on ISMS	Mitigation strategies
External				
Political Stability	Political stability or instability in regions where the organization operates can affect regulatory compliance and business continuity.	High	Delays in compliance activities	diversify geographical presence
Environmental Disasters	Natural disasters (e.g., earthquakes, floods) can disrupt data centers and operations	High	Data loss, downtime, and service disruptions	Implement robust disaster recovery and business continuity plans, regularly test them.
Technological Advancements	Rapid technological advancements may require adjustments to cybersecurity measures and tools	High	Need for ongoing training and technology updates	Invest in continuous employee training and cybersecurity technology
Economic Downturn	Economic downturns can affect budget allocation for information security and cybersecurity investments	Moderate	Budget constraints, reduced ability to implement new security measures	Prioritize critical security measures within budget constraints
Regulatory Changes	Changes in data protection and privacy regulations require adjustments to compliance measures	High	Need for policy and procedure updates, potential legal consequences for non-compliance	Regularly monitor regulatory changes and update policies accordingly
Internal				
Staff skills	Ensuring that employees are well-informed about data security best practices and are aware of potential threats	High	Reduced risk awareness, non-compliance with security policies	Conduct ongoing employee training and awareness programs
Resource Constraints	Limited budget and human resources for information security initiatives	High	Limitations on security investments, potential understaffing	Prioritize security initiatives, consider outsourcing where feasible
…….	…….	…….	…….	…….
…….	…….	…….	…….	…….
…….	…….	…….	…….	…….

2) Do you have a way to regularly review and monitor the changes made to these issues?

How to do :

Step	Description
Establish a Review Schedule	Define a schedule for reviewing external and internal issues at regular intervals.
Designate Responsibility	Assign responsibility for monitoring and reviewing issues to a specific individual within the organization.
Identify Data Sources	Identify reliable sources of information for each category of issue, including government websites, industry publications, internal audits, and feedback channels.
Document Changes	Maintain a centralized repository for documenting changes to issues
Regular Review Meetings	Conduct regular review meetings or workshops to discuss changes and invite input from stakeholders.
Training and Awareness	Ensure employees and stakeholders are aware of the importance of monitoring and provide training to contribute effectively.

Example of the review schedule :

- **Quarter 1: January - March**
  - **External Issues**:
    - Political Stability: Review political stability in regions and its impact on regulatory compliance.
    - Regulatory Changes: Check for any new data protection or financial regulations.
  - **Internal Issues**:
    - Employee Awareness and Training: Review the effectiveness of ongoing training programs for cybersecurity awareness.
- **Quarter 2: April - June**
  - **External Issues**:
    - Technological Advancements: Assess recent technological advancements and their relevance to cybersecurity.
    - Economic Downturn: Monitor economic conditions and their potential impact on budgets.
  - **Internal Issues**:
    - Resource Constraints: Evaluate the budget allocation for information security initiatives.
- **Quarter 3: July - September**
  - **External Issues**:
    - Changing Social Trends: Analyze evolving social attitudes and customer expectations related to data security.

        - Environmental Disasters: Review the organization's disaster recovery plans.
    - **Internal Issues**:
        - Compliance with Security Policies: Audit compliance with internal security policies and procedures.
- **Quarter 4: October - December**
    - **External Issues**:
        - Political Stability: Re-evaluate the political stability in regions of operation.
        - Regulatory Changes: Review changes to data protection and privacy regulations.
    - **Internal Issues**:
        - Employee Awareness and Training: Conduct employee awareness campaigns and training updates.

Example of identifing Data Sources :

- **Government Websites**:
    - *External Issues*: Political Stability and Regulatory Changes.
    - *Description*: Official government websites, provide information on political stability and regulatory changes that may impact the organization's cybersecurity operations.
- **Industry Publications**:
    - *External Issues*: Technological Advancements, Changing Social Trends.
    - *Description*: Subscriptions to industry-specific magazines, journals, and online publications.
- **Market Research Reports**:
    - *External Issues*: Economic Downturn.
    - *Description*: Market research reports from reputable firms provide insights into economic trends and their potential impact on the demand for cybersecurity services.

Exercise 7: Identifying External and Internal Issues for an ISMS

Scenario: Imagine you work for a medium-sized e-commerce company, "SecureMart." SecureMart is looking to implement ISO 27001-compliant information security management practices. Your task is to identify external and internal issues that are relevant to SecureMart's ISMS.

Instructions: For this exercise, identify at least three external issues and three internal issues that are relevant to SecureMart's ISMS. Provide a brief explanation of each issue.

External Issues:

1. **Legal and Regulatory Changes**:
    - *Explanation*: SecureMart operates in multiple countries, and there are frequent changes in data protection laws and regulations. Staying compliant with evolving legal requirements is crucial for the company's ISMS.
2. **Competitive Landscape**:
    - *Explanation*: Understanding the competitive landscape is essential as SecureMart's competitors are constantly evolving. Competitors could pose security risks, such as launching cyberattacks to gain a competitive advantage.

Internal Issues:

1. **Employee Awareness and Training**:
    - *Explanation*: Employee knowledge and awareness about information security are essential. Ensuring that employees understand their roles in maintaining security is an internal issue that impacts the ISMS.
2. **Resource Constraints**:
    - *Explanation*: SecureMart faces resource constraints in terms of budget and IT personnel. These constraints can affect the company's ability to implement and maintain robust security measures.
3. **Security Policy Compliance**:
    - *Explanation*: Adherence to security policies and procedures by employees is a vital internal issue. The effectiveness of security controls relies on employees following established policies.

Solution:

The exercise demonstrates the identification of external and internal issues relevant to SecureMart's ISMS:

- **External Issues**: Legal and regulatory changes, the cybersecurity threat landscape, and the competitive landscape are all external factors that can directly impact SecureMart's ISMS. Staying informed about these issues is crucial for the security of customer data and the e-commerce platform.
- **Internal Issues**: Employee awareness and training, resource constraints, and security policy compliance are internal issues within the organization. Addressing these issues is essential for ensuring that employees are educated about security practices, that the company allocates adequate resources for security, and that policies are effectively enforced.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:
a) interested parties that are relevant to the information security management system; and
b) the requirements of these interested parties relevant to information security.

- Start by conducting a stakeholder analysis. This involves identifying and categorizing all the individuals, groups, or organizations that have an interest in your information security. This can include :

- **Customers :**
  An effective ISMS assures them that their data and transactions are secure, which can build trust and loyalty.

- **Employees**
  A well-implemented ISMS provides employees with the tools and training to contribute to a secure sensitive company information.

- **Suppliers and partners**
  Suppliers and partners rely on the organization for various aspects of their business.
  They are interested in the security of shared data.
  A robust ISMS ensures that shared information is secure.

- **Regulators and government agencies**
  Regulators are deeply concerned about compliance with laws and regulations, especially those related to data protection and privacy.
  They have the authority to impose fines and penalties for non-compliance.
  A well-structured ISMS ensures adherence to relevant regulations.

- **Industry associations**

  Industry associations often set standards and best practices for information security.

  They may be interested in how well your organization aligns with those standards.
  Complying with industry standards enhances credibility within the sector.

- **Competitors**

  Competitors may have a general interest in your organization's security practices and could potentially exploit vulnerabilities.
  Protecting sensitive business information and trade secrets is a significant concern.
  A robust ISMS helps safeguard critical business data from Competitors.

- **Legal authorities**

  Legal authorities have a significant interest in ensuring that your organization complies with relevant laws.
  Non-compliance can result in legal actions and penalties.
  An ISMS helps demonstrate adherence to legal requirements.

- **Media**

  The media can affect an organization's reputation significantly.
  They are interested in security incidents, data breaches, and the organization's response to these events.
  An effective ISMS can help mitigate reputational damage.

- **Internal audit and compliance teams**

  These teams are responsible for ensuring that the organization meets its internal policies and industry standards.
  They are deeply interested in how well the ISMS aligns with these standards.
  An ISMS streamlines internal compliance processes.

➔ **These expectations will help you create a successful ISMS**

Exercise :

Organization Context:

ABC Financial Services is a financial institution specializing in providing a range of banking and financial products to individual customers and small businesses. The organization has a network of branches, a significant online presence, and a mobile app for customers to access their accounts and conduct transactions. They handle a sensitive customer financial data.

Scope of ISMS: The scope of the ISMS is to manage and secure all information assets related to customer financial data, operational processes, and IT infrastructure. The ISMS is designed to ensure the confidentiality, integrity, and availability of customer data and maintain compliance with financial industry regulations.

Task : Identifying External and Internal Issues

Solution :

- **Identify External Issues:**
    - Brainstorm with your functional team to identify external factors that can impact your ISMS. These may include:
        - Changes in financial industry regulations (e.g., introduction of new data protection laws).
        - Increased cyber threats targeting financial institutions.
        - Economic conditions affecting the financial sector.
        - Emerging technologies (e.g., blockchain, AI) that may impact the banking industry.
    - Discuss and list these external issues.

Identify Internal Issues:

- Brainstorm to identify internal factors that can impact your ISMS, such as:
    - Insufficient cybersecurity budget.
    - Lack of employee training on data security practices.
    - Recent acquisition or merger.
    - Rapid growth of online customer transactions.
    - Organizational culture (e.g., resistance to change).

Evaluation of 4.2:

1) Have you determined the needs and expectations of interested parties regarding your ISMS and are you reviewing them regularly ?

How to do :

Step 1: Identify Key Stakeholders

- Identify and list the key stakeholders relevant to your ISMS. In the case of ABC Financial Services, this could include customers, shareholders, regulators, employees, cybersecurity partners, external auditors, IT suppliers, legal authorities, competitors, and industry associations.

Step 2: Categorize Stakeholders

- Categorize these stakeholders based on their significance and potential impact on the ISMS. You can use a stakeholder power-interest grid, like the one below:

Stakeholder Category	Description
High Power, High Interest	e.g., Regulators, Shareholders
High Power, Low Interest	e.g., Cybersecurity Partners
Low Power, High Interest	e.g., Employees, Customers
Low Power, Low Interest	e.g., Competitors, Industry

Step 3: Data Collection and Analysis

- Conduct regular surveys or interviews with key stakeholders to gather their needs and expectations related to information security.

Step 4: Document and Analyze Findings

- Document the findings from these data collection efforts. Create a comprehensive report that outlines the needs and expectations of each stakeholder category.

Step 5: Regular Review and Update

- Schedule regular reviews of the documented needs and expectations. This should be part of your ISMS review process, which could be done on an annual basis or as required.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

Determining the scope of an Information Security Management System (ISMS) in the is a critical initial step. It sets the boundaries of the ISMS. This includes identifying the information assets, processes, and locations relevant to information security.
The process of defining the scope is :

Identify Stakeholders

Identify the stakeholders who have an interest in the ISMS. These may include clients, employees, regulatory bodies, and suppliers.

Determine Business Objectives

Such as delivering high-quality software, meeting client expectations, and maintaining a competitive edge. Understanding these objectives helps in defining the scope.

Assess Legal and Regulatory Requirements

The organization identifies the legal and regulatory requirements that are applicable to their operations. For example, they identify data protection laws.

Map Information Assets

Determine the critical information assets that are part of the ISMS. For example source code, client data, intellectual property, and sensitive internal documents.

Evaluate Processes

Evaluate the business processes that interact with or impact the identified information assets. This helps determine which processes fall within the scope of the ISMS. For example software development, data storage, and client communication processes.

Define Locations

Identify the geographical locations where the organization operates. This could be multiple office locations, data centers, or cloud providers. Each location has its security implications and should be part of the scope.

Consider Interfaces

Identify any external interfaces where information is shared with third parties. For example client communication channels and data transfer interfaces with suppliers.

Document the Scope Statement

Based on the information gathered, creates a scope statement that defines the boundaries of the ISMS. This statement may include:

- A clear description of the scope, such as "The scope of the ISMS encompasses all software development and client data handling processes, systems, and assets within XYZ organization, including its offices in the US and India."
- A list of the specific locations and processes included in the scope.
- A mention of the applicable legal and regulatory requirements.
- A description of any external interfaces or third-party relationships that impact the ISMS.

Example of scope

« The scope of our ISMS encompasses the protection of sensitive customer data, software source code. This includes all office locations and data centers »

Exercice :

XYZ Healthcare is a leading healthcare provider with multiple hospitals, clinics, and healthcare centers. They manage sensitive patient healthcare records, financial data, and rely on various IT systems for their operations. Data security is critical for patient privacy, compliance with healthcare regulations (e.g., HIPAA), and ensuring the continuity of medical services.

Task : To define the scope of the ISMS for XYZ Healthcare.

Solution :

Steps:

1. **Identify Key Information Assets:** Start by listing the critical information assets that the ISMS must protect. In the case of XYZ Healthcare, these may include electronic health records (EHRs), patient billing information, medical research data, and hospital administration records.
2. **Identify Business Processes:** Determine the core business processes and activities that involve or affect the identified information assets. These could be patient admissions, medical treatment, billing, and data management.
3. **Identify Locations:** Consider all the locations where these information assets and processes are managed. This may include hospitals, clinics, data centers, and remote offices.
4. **Regulatory Considerations:** Identify the relevant legal and regulatory requirements that impact XYZ Healthcare, such as HIPAA (Health Insurance Portability and Accountability Act) and other healthcare-specific regulations.
5. **Interfaces and Partners:** Identify any external interfaces with third-party service providers, such as healthcare software vendors, cloud service providers, and insurance companies. These interfaces need to be within the scope.
6. **Document the Scope Statement:** Create a concise scope statement, including a clear description of what is included and excluded. For example: "The scope of the ISMS includes all electronic health records (EHRs), patient billing data, and associated processes within XYZ Healthcare's hospitals, clinics, data centers, and remote offices. It encompasses compliance with HIPAA regulations and extends to third-party interfaces and service providers. Excluded from the scope are non-healthcare-related data and processes, and physical security measures."

Evaluation of 4.3:

How the scope of the ISMS clearly defined and documented ?

5 - Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system.

The following activities represent management commitment:

a) stablishing information security policy

b) ensuring availability of resources necessary for the ISMS (financial resources, dedicating people, allocating time, …) for information security activities

c) communicating the importance of information security

d) promoting continual improvement of the ISMS (enabling employees to propose improvements through suggestion boxes, dedicated email, discussion group, brainstorming sessions, …)

Stablishing information security policy

Defining and documenting the organization's information security policy and setting clear information security objectives.

The organization must create and document an information security policy. This policy is a high-level statement of management's intent and commitment to information security. It provides a framework for setting information security objectives and is based on the organization's risk assessment and legal requirements.

The information security policy should align with the organization's overall business objectives and the needs.

These objectives are derived from the organization's risk assessment and are designed to address identified risks and opportunities.

Information security objectives should be measurable, meaning they can be quantified or assessed to determine whether they are being achieved. These measurable objectives help in evaluating the effectiveness of the ISMS.

Each objective should have a clear assignment of responsibility. This ensures that specific individuals or roles are accountable for achieving these objectives.

Communication

The policy must be communicated within the organization, ensuring that all employees and relevant stakeholders are aware of its existence and their responsibilities related to information security.

Review and Update

The information security policy should be reviewed regularly to ensure its continued relevance and effectiveness. Any necessary updates or changes should be made as the organization's context evolves.

Establishing the information security policy and objectives is not a one-time effort. Continuous improvement is a key principle of ISO 27001. The organization should regularly monitor and review the policy and objectives to adapt to changing risks and opportunities and ensure ongoing alignment with business objectives.

5.2 policy

Top management shall establish an information security policy

Top management is responsible for an infomation security policy and distribute it to all the employees in the company and make it available to appropiate interested parties

° this policy should include the intentions of the company regarding information security

° should show the management commitment and continually improve the ISMS

° give the directions for setting information security objectives

° it is important because it sets the basis of ISMS and gives the direction in which the ISMS will be developed and maintained

° is a top level policy and shouldn’t be too detailed (the details about controls and rules in other lower level documents like detailed policies and procedures)

Example of security policy :

1. Introduction

1.1 Policy Statement: XYZ organization is committed to ensuring the confidentiality, integrity, and availability of all information assets and systems. This Information Security Policy outlines our organization's commitment to information security, the responsibilities of employees and stakeholders, and the framework for managing information security risks. We aim to comply with all relevant legal and regulatory requirements and continually improve our information security practices.

1.2 Policy Purpose: The purpose of this policy is to provide a framework for information security management, promoting best practices, and mitigating risks associated with the use of information and information systems within the organization.

2. Scope

2.1 Policy Scope: This policy applies to all employees, contractors, third-party suppliers, and any other individuals or entities accessing or managing XYZ organization’s information assets and systems.

2.2 Policy Exclusions: This policy does not cover information assets not owned by XYZ organization or information systems used for personal purposes, not related to company operations.

3. Information Security Objectives

3.1 Objectives: XYZ organization establishes the following information security objectives to guide our efforts:

- Ensure the confidentiality and privacy of sensitive information.
- Maintain the integrity and accuracy of data.
- Guarantee the availability and reliability of critical information systems.
- Comply with relevant legal and regulatory requirements, including data protection and industry-specific regulations.
- Educate and engage all employees in information security best practices.
- Continuously monitor and improve our information security measures.

4. Information Security Responsibilities

4.1 Management Commitment: Top management is committed to information security and providing the necessary resources to establish, implement, and maintain an effective Information Security Management System (ISMS).

4.2 Employee Responsibilities: All employees are responsible for safeguarding information assets, reporting security incidents, and complying with security policies and procedures.

4.3 Information Security Officer (ISO): The ISO is responsible for overseeing the ISMS, coordinating security activities, and ensuring compliance with security policies and standards.

4.4 Data Owners and Custodians: Data owners are responsible for classifying data, and data custodians are responsible for implementing access controls and protecting data in accordance with classifications.

5. Information Security Controls

5.1 Access Control: Access to information systems and data is restricted based on user roles and responsibilities. Access is granted only to authorized individuals.

5.2 Data Protection: Sensitive data is classified, and appropriate safeguards are implemented to protect its confidentiality, integrity, and availability. Encryption is used for sensitive data in transit and at rest.

5.3 Incident Response: A documented incident response plan is in place to address and report security incidents promptly.

5.4 Security Awareness and Training: Employees are provided with information security awareness and training to ensure they understand and follow security policies and best practices.

5.5 Compliance and Audit: Regular compliance assessments, audits, and security reviews are conducted to ensure the effectiveness of information security controls.

6. Continuous Improvement

XYZ organization is committed to ongoing improvement of information security practices and the ISMS. This policy will be reviewed annually and updated as necessary to align with the evolving threat landscape, business operations, and legal requirements.

Example of ensuring ressources :

Context: ABC Tech Solutions is an IT services company that provides software development and IT consulting services to clients. They are implementing ISO 27001 to enhance information security.

Step 1: Resource Assessment

- **Identify ISMS Resource Requirements:** Begin by identifying the resources required for the ISMS. These resources may include personnel, technology, physical infrastructure, and financial resources. For example, ABC Tech Solutions may need security professionals, access control systems, secure storage facilities, and a budget for training and security tools.

Step 2: Resource Allocation

- **Budget Allocation:** Allocate a budget for the ISMS. This should cover expenses related to hiring or training security personnel, acquiring security software/tools, and any other investments needed to maintain the ISMS.
- **Personnel Assignment:** Appoint or hire personnel responsible for information security. This might include a Chief Information Security Officer (CISO) or Information Security Manager. These individuals will oversee the ISMS and ensure resources are appropriately allocated.

Step 3: IT Infrastructure and Technology

- **Secure Infrastructure:** Invest in or upgrade IT infrastructure to ensure the availability and integrity of information. This could include redundancy in data centers, regular backups, and disaster recovery systems to maintain the availability of critical systems.
- **Security Software:** Invest in security software, such as firewalls, intrusion detection systems, and encryption tools, to protect information assets and ensure their availability.

Step 4: Training and Awareness

- **Staff Training:** Allocate resources for training employees on information security best practices. This includes regular training sessions and workshops to enhance their awareness of security risks and how to mitigate them.
- **Communication:** Develop and distribute information security policies and guidelines to all employees, ensuring they are aware of their responsibilities in maintaining information security.

Step 5: Periodic Review and Maintenance

- **Regular Resource Evaluation:** Continuously review the allocation and utilization of resources to ensure they align with the evolving needs of the ISMS.

- **Budget Reassessment:** Regularly assess the budget allocation to ensure that it remains adequate to support the ISMS's resource requirements.
- **Technology Updates:** Stay updated with technological advancements and ensure that the organization's security tools and infrastructure are current and effective.

Step 6: Contingency Planning

- **Resource Contingency Planning:** Develop contingency plans to address unexpected events that may impact the availability of resources. This includes plans for resource reallocation in case of budget constraints or disruptions in IT infrastructure.

Step 7: Documentation

- **Resource Allocation Records:** Maintain clear and up-to-date records of how resources are allocated for the ISMS. This includes budget documentation, personnel assignments, and details about technology and infrastructure investments.

Example of Resource Allocation Record

Resource Type	Resource Description	Responsible Person	Allocation Date	Budget Allocation (USD)	Actual Expenditure (USD)
Personnel	CISO - Chief Information Security Officer	John Doe	01/01/2023	$150,000	$147,500
Personnel	Security Analyst	Jane Smith, Analyst	01/15/2023	$80,000	$82,500
Infrastructure	Data Center Redundancy	IT Department	02/01/2023	$250,000	$245,000
Technology	Firewall Upgrade	IT Department	02/15/2023	$30,000	$28,500
Training	Employee Security Training	HR Department	03/01/2023	$10,000	$10,000

Explanation:

- **Resource Type:** This column specifies the type of resource being allocated. Resources can include personnel, infrastructure, technology, training, and more.
- **Resource Description:** This column provides a brief description of the resource, including the position for personnel, equipment for infrastructure, or specific technology or training program.
- **Responsible Person:** The individual or department responsible for managing the allocated resource.
- **Allocation Date:** The date on which the resource allocation was initiated.
- **Budget Allocation (USD):** The budgeted amount allocated for the resource.
- **Actual Expenditure (USD):** The actual amount spent or utilized. This should be periodically updated to reflect expenditures accurately.

Example: Communication of Information Security Importance

Message: "Securing Our Financial Services, Protecting Our Clients"

Audience: All Employees at XYZ Financial Services

Delivery Method: Company-wide email from the CEO

Subject: Prioritizing Information Security

Message:

Dear Team,

I want to take a moment to emphasize the critical role each one of us plays in ensuring the security of our financial services and, more importantly, safeguarding our clients' trust.

In today's digital age, the importance of information security cannot be overstated. As a financial services provider, we are entrusted with sensitive financial and personal data, and our clients rely on us to keep this information safe from harm. The repercussions of a security breach could be devastating to our clients and our reputation.

Here are some key points to consider:

1. Client Trust: Our clients trust us with their financial well-being. Information security is the foundation of this trust. Protecting their data is not just a legal requirement; it's a moral obligation.

2. Regulatory Compliance: Compliance with financial industry regulations (e.g., GDPR, HIPAA) is mandatory. Non-compliance can result in legal consequences and financial penalties.

3. Business Continuity: A security breach can disrupt our operations, leading to downtime, financial losses, and damage to our reputation. Our competitors are just a click away, and clients have options.

4. Reputation: Our reputation is one of our most valuable assets. Security incidents can tarnish our image and lead to a loss of clients' trust.

5. Personal Responsibility: Each of us plays a vital role in information security. Whether you work in IT, customer service, or administration, your actions have an impact.

6. Continuous Learning: Information security is an evolving field. We encourage you to stay updated on security best practices through our training programs and awareness initiatives.

Remember, security is not just the responsibility of our IT department; it's everyone's responsibility. We must all be vigilant and proactive in identifying and mitigating security risks.

Please take this message to heart and consider it a call to action. Our commitment to information security is unwavering, and it is fundamental to our long-term success. I encourage you to reach out to our dedicated security team if you have any questions or concerns.

Thank you for your dedication to our clients and our organization's success.

Sincerely,

[CEO's Name]

Context: XYZ Financial Services is a financial institution that has implemented ISO 27001 to enhance its information security. Promoting continual improvement is crucial for maintaining a robust ISMS.

Example of Promoting Continual Improvement:

1. **Regular Risk Assessment and Management:**
    - **Practice:** XYZ Financial Services conducts regular risk assessments to identify new threats, vulnerabilities, and changing business conditions that may affect information security.
    - **Implementation:** The organization uses automated risk assessment tools to identify and assess potential risks. Additionally, they periodically engage with external security experts to provide fresh perspectives on emerging threats.
    - **Outcome:** By continuously assessing risks and vulnerabilities, XYZ Financial Services identifies areas for improvement in its ISMS. They can then make informed decisions about resource allocation and control enhancements to mitigate these risks.
2. **Security Incident Response and Analysis:**
    - **Practice:** XYZ Financial Services has established an incident response team that follows a well-defined incident response plan. They investigate and analyze security incidents.
    - **Implementation:** The incident response team holds post-incident meetings to discuss lessons learned and identifies areas where security controls can be strengthened to prevent similar incidents in the future.
    - **Outcome:** This continual improvement approach ensures that the organization's response to security incidents becomes increasingly effective. By learning from each incident, they refine their procedures and controls to enhance security.
3. **Regular Audits and Reviews:**
    - **Practice:** XYZ Financial Services conducts regular internal and external audits of their ISMS to assess compliance with ISO 27001 standards and internal policies.
    - **Implementation:** The audit findings are discussed in management review meetings. Any non-conformities or areas for improvement are documented and tracked.
    - **Outcome:** Through this process, XYZ Financial Services identifies areas where the ISMS can be strengthened and takes corrective and preventive actions to address non-conformities. This contributes to the overall
    - improvement of the ISMS.

4. **Employee Training and Awareness:**
    - **Practice:** XYZ Financial Services provides regular information security training to employees and raises awareness through communication and training programs.
    - **Implementation:** Feedback from employees and security incident reports is used to refine and improve training content. Additionally, the organization encourages employees to report security concerns and suggests improvements.
    - **Outcome:** The continuous feedback loop with employees leads to more relevant and effective training programs. Employees become more proactive in identifying security risks, which contributes to a culture of continuous improvement in security awareness.
5. **Benchmarking and Best Practices:**
    - **Practice:** XYZ Financial Services actively participates in industry forums, shares information with peer organizations, and keeps updated on emerging security trends and best practices.
    - **Implementation:** The organization regularly reviews industry benchmarks and case studies and implements relevant best practices in its ISMS.
    - **Outcome:** By benchmarking against peers and adopting industry best practices, XYZ Financial Services ensures that its ISMS remains aligned with the latest security standards and continuously evolves to meet new challenges.

Promoting continual improvement in these ways helps XYZ Financial Services maintain the effectiveness and relevance of its ISMS. It's a dynamic process that ensures the organization is proactive in addressing emerging security threats and evolving with changing business and regulatory landscapes.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated

° Top management must define the roles and responsabilities for information security

° Top management must communicate those responsabilities to everyone in the organization

° It is important (employees will know what is expected of them, how can they contribute)

° Top management should assign two types of responsibilities :

- responsabilities for ensuring implementation of ISMS according to ISO 27001

- responsabilities for monitoring the performance of the ISMS and reporting to top management

Context: XYZ Corporation is a mid-sized technology company that is committed to implementing ISO 27001 to strengthen its information security management system.

Top Management Responsibilities:

CEO (Chief Executive Officer) - John Smith:

- Responsible for demonstrating leadership and commitment to the ISMS and ensuring that information security aligns with business goals.

CFO (Chief Financial Officer) - Sarah Johnson:

- Responsible for allocating financial resources for the ISMS, including budgeting for information security initiatives.

CIO (Chief Information Officer) - David Patel:

- Responsible for overseeing the overall information security program, including policy development and risk management.

CISO (Chief Information Security Officer) - Emily Brown:

- Responsible for the design, implementation, and monitoring of the ISMS.
- Leads the information security team and ensures compliance with ISO 27001 standards.
- Reports directly to the CEO and provides regular updates on the status of the ISMS.

HR Director - Mark Lewis:

- Responsible for ensuring that all employees receive security awareness training.
- Collaborates with the CISO to develop and implement security policies and guidelines.
- Manages personnel security aspects, including background checks and clearances.

IT Manager - Lisa Rodriguez:

- Responsible for the day-to-day management of IT security operations, including network security, system hardening, and security incident response.
- Collaborates with the CISO to ensure that IT security practices align with the ISMS.

Legal Counsel - Alex Turner:

- Ensures legal compliance with data protection and privacy laws, and that contractual agreements with third parties include information security clauses.

Business Unit Heads - Sarah Hughes (Marketing), Michael Chen (Sales), Rachel Patel (Product Development), James Wilson (Operations):

- Responsible for implementing security measures within their respective business units and ensuring that employees are aware of and follow security policies.
- Report to the CISO on information security issues and compliance within their areas of responsibility.

Compliance Manager - Daniel Foster:

- Responsible for monitoring and ensuring compliance with ISO 27001 standards and legal requirements.
- Reports to the CISO and conducts regular internal audits to verify compliance.

Communication and Awareness Officer - Susan Carter:

- Responsible for developing and executing security awareness programs for all employees.
- Collaborates with HR and the CISO to ensure ongoing security training and communication.

Risk Management Specialist - Kevin Ward:

- Responsible for conducting risk assessments and helping the organization identify and mitigate information security risks.
- Works closely with the CISO to ensure risks are addressed in the ISMS.

Facility Manager - Michelle Adams:

- Ensures the physical security of the organization's premises and data centers.
- Collaborates with the IT department to ensure the security of physical access to critical areas.

6 - Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2

When planning for the Information Security Management System (ISMS), it is essential for the organization to consider the issues referred to in 4.1 and the requirements referred to in 4.2

1. Issues Referred to in 4.1 - Understanding the Organization and its Context:

ISO 27001 Clause 4.1 requires the organization to consider issues related to its internal and external context.

Internal Context: Understand the internal issues, which can encompass factors like organizational culture, structure, policies, and resources. This includes understanding the organization's values, its strategic direction, and its current practices related to information security

External Context: Consider external issues that might impact the organization's information security, such as legal and regulatory requirements, industry standards, stakeholder expectations, and changes in the business environment. It's crucial to be aware of the legal and regulatory landscape that may affect data protection and privacy

2. Requirements Referred to in 4.2 - Understanding the Needs and Expectations of Interested Parties:

ISO 27001 Clause 4.2 focuses on understanding the needs and expectations of interested parties, particularly as they relate to information security. These interested parties can include customers, regulators, business partners, and employees

Identifying Interested Parties: Recognize who the relevant interested parties are and determine their specific information security needs and expectations. For example, customers may expect data privacy, while regulators may have specific compliance requirements

Understanding Needs and Expectations: Investigate and gather information on the needs and expectations of these parties. This can be done through surveys, consultations, feedback mechanisms, and analysis of regulatory requirements and industry standards

Examples :

- By understanding the needs and expectations of employees (4.2), you can identify the importance of security training and awareness programs to mitigate risks related to human error.
- By understanding the needs and expectations of interested parties (4.2), including regulators, you can identify their specific requirements to avoid legal fees, fines, …
- Understanding the needs and expectations of third-party vendors and suppliers (4.2) can help assess the risks associated with their services, including data breaches or service interruptions.
- Understanding the needs and expectations of customers and data subjects (4.2) can reveal the importance of data privacy. This aids in risk assessment and compliance with data protection regulations.
- By understanding the needs and expectations of competitors (4.2), you can assess the potential risks associated with cyber-espionage, data theft, or industrial sabotage.
- Understanding the needs and expectations of technology partners and IT service providers (4.2) helps in identifying technological risks such as vulnerabilities in software.
- By understanding the needs and expectations of shareholders and investors (4.2), you can assess financial risks tied to information security incidents that may impact the organization's value
- Understanding the needs and expectations of customers and the general public (4.2) can help assess risks related to data breaches that may damage the organization's reputation.

Stakeholder	Needs and Expectations	Associated Risks	Risk Mitigation Measures
Customers	Data privacy, security, reliable services	Data breaches, service interruptions, loss of trust	Implement strong data encryption, redundancy for service continuity, regular security audits, and transparent data handling policies.
Regulators	Compliance with industry regulations	Non-compliance penalties, legal actions, reputation damage	Regular compliance audits, legal counsel, and proactive adherence to regulations.
Employees	Secure work environment, training and awareness	Insider threats, negligence, security incidents	Security training, clear policies and procedures, user access control, and incident response plans.
Shareholders	Return on investment, corporate responsibility	Financial losses, damage to reputation, regulatory non-compliance	Transparent reporting, adherence to ethical practices, and risk management strategies.
Business Partners	Secure data exchange, compliance with agreements	Data breaches, contractual disputes, loss of partnerships	Secure data transfer protocols, contractual compliance, and dispute resolution processes.
Competitors	Protection of proprietary information	Data theft, industrial espionage, competitive disadvantage	Secure proprietary information, monitoring for unauthorized access, and legal action if necessary.
Technology Providers	Secure integration, adherence to service levels	Service disruptions, data leaks, contractual disputes	Secure integration protocols, service-level agreements (SLAs), and contingency plans for service disruptions.
Regulatory Bodies	Compliance with legal and regulatory standards	Non-compliance penalties, legal actions, loss of operating licenses	Ongoing monitoring of regulatory changes, legal compliance teams, and regular assessments.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;

Risk acceptance is a concept in risk management that involves acknowledging and agreeing to the existence of a specific risk without taking further action to mitigate it. When an organization or individual accepts a risk, they are essentially making an informed decision that the potential negative consequences or impacts of that risk are either:

1. Tolerable: The organization is willing to live with the risk because the potential harm, should it occur, is considered manageable or within acceptable limits. In such cases, the organization has determined that the cost or effort required to mitigate the risk is greater than the expected impact.

   Examples

   Software Bugs in Non-Critical Systems: An organization may accept the risk of software bugs in non-critical internal applications. While these bugs may cause occasional inconveniences, the cost of exhaustive testing and bug-fixing for non-critical systems may be deemed too high

   Employee Errors in Non-Critical Documentation: In an office setting, the risk of minor errors in non-critical documents or reports may be tolerated. While perfection is ideal, the time and resources required to prevent all minor errors in routine documentation might not be justifiable.

   Temporary Network Congestion: An organization might accept temporary network congestion during peak usage times, understanding that the costs of building additional network infrastructure to prevent congestion are higher than the occasional slowdown

2. Unavoidable: The risk may be accepted because it is beyond the organization's or individual's control, and there are no practical or cost-effective measures to reduce the risk further.

   Examples

   Natural Disasters: Some natural disasters, such as earthquakes or tsunamis in earthquake-prone regions, are generally unavoidable. While organizations can take measures to mitigate the impact, the fundamental risk remains.

More detailed risk acceptance criteria :

Risk Statement	Risk Acceptance Criteria	Examples of Risks That Meet Criteria
Unauthorized Access to Non-Critical Systems	- If data exposed is non-sensitive and of minimal value. - If data integrity remains intact. - If there's no significant impact on availability. - If the likelihood is very low due to strong security controls. - If no legal or regulatory compliance issues arise.	Unauthorized access to a non-critical internal wiki. Unauthorized access to a development server with non-sensitive data.
Temporary Service Disruptions	- If service interruptions have minimal impact on business operations. - If there's no critical data loss or reputational damage. - If service recovery is swift.	Temporary network downtime not affecting critical operations. Brief email server outage with minimal impact.
Employee Mistakes Leading to Non-Critical Data Loss	- If the data lost is non-sensitive and holds no strategic value. - If data integrity remains intact. - If no significant legal or regulatory compliance issues arise.	Accidental deletion of non-sensitive non-critical data. Employee error leading to non-critical data misplacement.
Low Severity Software Vulnerabilities	- If the identified software vulnerabilities have low severity and pose minimal risk. - If patches or mitigations are available and can be promptly applied.	Discovery of low-severity software vulnerabilities with readily available patches.
Minor Third-Party Vendor Risks	- If third-party vendor risks are identified as low impact. - If contractual agreements with vendors offer protection.	Minor operational disruption due to a non-critical vendor's temporary service issue.
Temporary Network Performance Issues	- If network performance issues have minimal impact on operations. - If performance returns to normal quickly.	Temporary network congestion leading to minor slowdowns in non-critical systems.
Minor Physical Security Breaches	- If the breach does not compromise sensitive assets or information. - If there's no significant reputational damage. - If corrective measures are promptly applied.	Unauthorized access to a non-critical office area with no theft or data exposure.

Criteria for performing information security risk assessments refers to the specific guidelines, standards, and factors that an organization or individual uses when evaluating and analyzing risks to information security. These criteria help ensure a structured and consistent approach to assessing and managing security risks.

Examples :

Table 1: Impact Criteria

Impact Level	Description
1	Negligible: Minimal impact, easily manageable, almost no disruption or loss.
2	Low: Limited impact, manageable with existing resources and controls, minor disruption or loss.
3	Moderate: Noticeable impact, requires additional resources or measures for mitigation, moderate disruption or loss.
4	High: Significant impact, major resources or efforts required for mitigation, severe disruption or loss.

Table 2: Likelihood Criteria

Likelihood Level	Description
1	Rare: Almost impossible to occur; occurrence is highly unlikely.
2	Unlikely: Possible, but not expected to occur except in exceptional circumstances.
3	Possible: Could occur occasionally under normal circumstances.
4	Likely: Expected to occur regularly or frequently under normal circumstances.

Table 3: Risk Assessment Matrix

Likelihood / Impact	1 (Negligible)	2 (Low)	3 (Moderate)	4 (High)
1 (Rare)	Low Risk	Low Risk	Moderate Risk	High Risk
2 (Unlikely)	Low Risk	Low Risk	Moderate Risk	High Risk
3 (Possible)	Low Risk	Moderate Risk	High Risk	High Risk
4 (Likely)	Moderate Risk	High Risk	High Risk	High Risk

- Identify risks associated with the loss of confidentiality, integrity and availability for information within the scope
- Identify the risk owners

Risks are related to the loss of confidentiality, and each example highlights a specific scenario where confidentiality may be compromised. Organizations need to assess and manage these risks as part of their information security management system in compliance with ISO 27001.

The "risk owner" is an individual or organization who is assigned the responsibility of managing a specific risk. The risk owner is accountable for various aspects of risk management, including mitigating, monitoring, and reporting on the risk. The concept of a risk owner is a fundamental component of an effective risk management framework. Here are the key responsibilities of a risk owner:

Mitigating or Managing the Risk: This may involve implementing controls, processes, or other measures to reduce the risk's impact or likelihood

Example: The CISO develops a plan to mitigate the risk by updating encryption protocols, implementing regular vulnerability assessments, and enhancing data access controls.

Monitoring the Risk: The risk owner continuously monitors the risk to ensure that the mitigation measures are effective and that the risk remains within acceptable levels. Regular monitoring helps identify changes in the risk landscape.

Example: The CISO continuously monitors the organization's network for any signs of security vulnerabilities or breaches using intrusion detection systems and logs analysis.

Reporting and Communication: The risk owner is responsible for communicating information about the risk to relevant stakeholders. This includes reporting on the status of the risk, any changes, and the effectiveness of mitigation measures.

Example: The CISO regularly reports to the executive team and the board of directors about the current status of cybersecurity risks, including the progress made in mitigating the identified risk.

Information Security Risk Assessment Table - Loss of Confidentiality

Risk Category	Risk Description	Example	Risk Owner
Unauthorized Access	Unauthorized access to sensitive data by an insider.	An employee with access privileges viewing sensitive HR record without authorization.	IT Security Team
Phishing Attacks	Phishing emails leading to data disclosure.	Employees falling victim to a phishing email, leading to the exposure of login credentials.	Security Awareness Team
Data Breach	External data breach exposing sensitive customer data.	A cyberattack leading to the theft of customer database containing personal information.	Data Protection Officer
Social Engineering	Social engineering attacks leading to data exposure.	A scammer impersonating IT support tricks an employee into sharing login credentials.	IT Security Team
Insider Threat	Insider threats compromising the confidentiality of data.	An employee copying sensitive data and selling it to a competitor.	HR Department
Data Theft	Theft of physical devices containing sensitive data.	A laptop containing sensitive financial data is stolen from an employee's car.	Data Protection Officer
Third-Party Vendor Risk	Third-party vendor experiencing security breaches.	A cloud service provider experiences a security breach, exposing customer data.	IT Support Team

Information Security Risk Assessment Table - Loss of Integrity

Risk Category	Risk Description	Example	Risk Owner
Unauthorized Data Modification	Unauthorized modification of critical data by an insider or external attacker.	An employee modifies financial records to embezzle funds.	IT Security Team
Data Corruption	Data corruption or data quality issues due to software errors, hardware failures, or transmission errors.	A software bug corrupts customer order data, resulting in incorrect shipments.	Security Awareness Team
Insider Threat	Insider threats compromising the accuracy and reliability of data, such as altering records or reports.	An employee with access changes sales data to inflate their commission.	Data Protection Officer
Tampering with Documents	Unauthorized alteration or tampering with important documents and records.	A supplier fraudulently alters contract documents to demand higher payments.	IT Security Team
Malicious Code Injection	Injection of malicious code into software or databases to compromise data integrity.	SQL injection attack alters a database, leading to unauthorized data changes.	HR Department
Unauthorized Software Installation	Unauthorized installation of software that introduces integrity risks.	An employee installs unapproved software with malware that manipulates files.	Data Protection Officer
Data Loss Prevention Failures	Failures in data loss prevention systems, leading to unauthorized data alterations or deletions.	A misconfigured DLP system accidentally alters customer data during monitoring.	IT Security Team
Falsification of Records	Intentional or unintentional falsification of records that impacts data integrity.	An employee unintentionally enters inaccurate safety records, affecting safety assessments.	Security Awareness Team

Hardware Component Failures	Failures of hardware components like hard drives or memory causing data corruption.	A server hard drive failure results in data corruption and loss of integrity.	Data Protection Officer
Poor Data Validation	Inadequate data validation during input, allowing for incorrect or unauthorized data entry.	A lack of input validation enables users to enter non-standard characters, affecting data integrity.	IT Security Team
Weak Access Controls	Weak access controls and user permissions leading to unauthorized data modifications.	An employee with excessive access rights changes critical data without proper authorization.	HR Department

Information Security Risk Assessment Table - Loss of Availability

Risk Category	Risk Description	Example	Risk Owner
Hardware Failure	Physical failure of critical server hardware	A server's hard drive fails, causing service downtime.	IT Security Team
Distributed Denial of Service (DDoS)	DDoS attack overwhelms network resources	A DDoS attack floods a web server with traffic, making it inaccessible.	Security Awareness Team
Network Outages	Network infrastructure failure or outage	An internet service provider experiences a network outage, disrupting connectivity.	Data Protection Officer
Power Outages	Unexpected power outage affecting data center	A power outage results in a data center going offline.	IT Security Team
Software Bugs	Software bugs causing system crashes or errors	A software bug causes an application to crash frequently.	HR Department
Data Corruption	Corruption of critical data or databases	A database becomes corrupted, rendering it unusable.	Data Protection Officer
Insider Threat	Insider threats compromising system availability	An employee intentionally disrupts network services.	Security Awareness Team
Third-Party Vendor Risk	Third-party vendor's service disruption	A cloud service provider experiences a service outage.	Data Protection Officer
Natural Disasters	Natural disasters like earthquakes, floods, or fires	A flood damages data center facilities, causing downtime.	IT Security Team
Configuration Errors	Misconfigurations leading to system unavailability	Misconfigured firewall rules disrupt network traffic.	HR Department
Human Error	Human errors causing system or service failures	An operator accidentally deletes critical data.	Data Protection Officer

- Assess the potential consequences that would result if the risks were to materialize;
- Assess the realistic likelihood of the occurrence of the risks and determine the levels of risk

Risks Associated with Loss of Confidentiality

Risk	Probability	Impact	Risk Level
Unauthorized Access	Medium	High	High
Phishing Attacks	Medium	High	High
Insider Threats	Low	High	Medium
Inadequate Access Controls	Medium	Medium	Medium

Risks Associated with Loss of Integrity

Risk	Probability	Impact	Risk Level
Data Tampering	Low	High	Medium
Software Vulnerabilities	Medium	High	High
Inadequate Change Control	Medium	Medium	Medium

Risks Associated with Loss of Availability

Risk	Probability	Impact	Risk Level
DDoS Attacks	Low	High	Medium
Hardware Failures	Low	Medium	Low
Power Outages	Low	Medium	Medium
Network Failures	Low	Medium	Low

- Compare the results of risk analysis with the risk criteria
- Prioritize the analysed risks for risk treatment.

Risk	Probability	Impact	Risk Level	Risk criteria
Unauthorized Access	Medium	High	High	High
Phishing Attacks	Medium	High	High	High
Software Vulnerabilities	Medium	High	High	High
Insider Threats	Low	High	Medium	Medium
Inadequate Access Controls	Medium	Medium	Medium	Medium
Data Tampering	Low	High	Medium	Medium
Inadequate Change Control	Medium	Medium	Medium	Medium
DDoS Attacks	Low	High	Medium	Medium
Power Outages	Low	Medium	Medium	Medium
Hardware Failures	Low	Medium	Low	Low
Network Failures	Low	Medium	Low	Low

- Select appropriate information security risk treatment option

Risk	Probability	Impact	Risk Level	Risk criteria	Action required
Unauthorized Access	Medium	High	High	High	Mitigation
Phishing Attacks	Medium	High	High	High	Mitigation
Software Vulnerabilities	Medium	High	High	High	Mitigation
Insider Threats	Low	High	Medium	Medium	Mitigation
Inadequate Access Controls	Medium	Medium	Medium	Medium	transfert
Data Tampering	Low	High	Medium	Medium	Mitigation
Inadequate Change Control	Medium	Medium	Medium	Medium	Mitigation
DDoS Attacks	Low	High	Medium	Medium	Mitigation
Power Outages	Low	Medium	Medium	Medium	transfert
Hardware Failures	Low	Medium	Low	Low	accepted
Network Failures	Low	Medium	Low	Low	accepted

- Determine all controls that are necessary to implement the information security risk treatment option(s) chosen

Risk	Probability	Impact	Risk Level	Risk criteria	Action required	controls
Unauthorized Access	Medium	High	High	High	Mitigation	° Access Control Policies ° Encryption ° Data Loss Prevention ° Security Awareness Training ° Intrusion Detection and Prevention Systems
Phishing Attacks	Medium	High	High	High	Mitigation	° Security Awareness Training ° Email Filtering and Anti-Phishing Solutions
Software Vulnerabilities	Medium	High	High	High	Mitigation	° Vulnerability Scanning and Patch Management
Insider Threats	Low	High	Medium	Medium	Mitigation	° Employee Background Checks ° User Activity Monitoring ° Data Access Auditing and Logging
Inadequate Access Controls	Medium	Medium	Medium	Medium	transfert	° Role-Based Access Control (RBAC) ° Two-Factor Authentication (2FA) ° Access Review and Recertification
Data Tampering	Low	High	Medium	Medium	Mitigation	° Data Backup ° Antivirus and Anti-Malware Solutions

						° Security Patch Management
Inadequate Change Control	Medium	Medium	Medium	Medium	transfert	
DDoS Attacks	Low	High	Medium	Medium	Mitigation	° DDoS Mitigation Solutions
Power Outages	Low	Medium	Medium	Medium	transfert	° Uninterruptible Power Supply (UPS)
Hardware Failures	Low	Medium	Low	Low	accepted	° Redundancy and Failover
Network Failures	Low	Medium	Low	Low	accepted	° Network Monitoring ° Redundant Network Architecture

- Compare the controls determined with those in Annex A and verify that no necessary controls have been omitted

Risk	Probability	Impact	Risk Level	Risk criteria	Action required	controls	Annex A Controls	Justification for Implementation	Justification for Exclusion
Unauthorized Access	Medium	High	High	High	Mitigation	° Access Control Policies	A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4	Access control policies are essential for defining who has access to what information.	none
						° Encryption	A.8.2.1, A.8.2.2, A.8.2.3, A.8.2.4	Encryption helps protect sensitive data during transmission and storage.	none
						° Data Loss Prevention	A.8.1.4, A.8.3.1, A.8.3.2	DLP solutions are necessary to prevent data leaks and unauthorized data	none

								transfers.	
						° Security Awareness Training	A.7.2.2, A.7.2.3, A.7.3.1	Security awareness training educates employees about risks, including phishing.	none
						° Intrusion Detection and Prevention Systems	A.12.4.1, A.12.4.3, A.12.4.4	IDPS helps detect and prevent unauthorized access and malicious activities.	none

- Formulate an information security risk treatment plan and obtain risk owners' approval of the Information security risk treatment plan and acceptance of the residual information security risks

Risk	Identified Controls	Risk Residual	Action Plan	Responsible	Target Completion Date
Unauthorized Access	1. Access Control Policies	Low	Implement access control policies.	IT Team	2023-01-15
	2. Encryption	Low	Implement encryption for sensitive data.	IT Team	2023-02-28
	3. Data Loss Prevention (DLP) Solutions	Low	Deploy DLP solutions for better data protection.	IT Team	2023-03-31
	4. Security Awareness Training	Medium	Conduct regular security awareness training.	HR/IT Team	Ongoing
	5. Intrusion Detection and Prevention Systems (IDPS)	Low	Deploy and maintain IDPS.	IT Team	2023-03-31

	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be communicated; and e) be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated

Information Security Objective	What Will Be Done	Resources Required	Responsible	Completion Date	(KPIs)
Enhance Access Control	- Review and update policies	- Access control software/hardware	IT Security Team	2023-03-15	- KPI 1: 100% compliance with updated access control policies. - KPI 2: 5 access control violations per quarter.
Conduct Security Awareness	- Develop training materials	- Training resources	HR/Training Team	Ongoing	- KPI 1: Average quiz score of 90% or higher in security awareness training. - KPI 2: 20% participants per quarter.
Enhance Incident Response	- Update incident response	- Incident response tools	IT Security Team	2023-04-30	- KPI 1: 100% success rate in trating incidents - KPI 2: Average time to resolve incidents within 2 hours.
……..	……..	……..	…….	……..	……..

7 - Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

The organization's responsibility is to determine and provide the resources needed for implementing an Information Security Management System (ISMS). These resources may include human resources, financial resources, technology, infrastructure, and any other assets needed to achieve the objectives of the ISMS. These ressources are :

- **Competent Personnel**: Ensure that personnel involved in information security activities are competent and possess the necessary skills and knowledge to effectively implement the ISMS. This may involve training, awareness programs, or hiring personnel with the required expertise.

- **Infrastructure and Technology**: Provide the necessary technological infrastructure and tools required to support the ISMS. This could include hardware, software, network resources, and other technical assets.

- **Financial Resources**: Allocate the necessary financial resources to cover the costs associated with the implementation and maintenance of the ISMS. This includes budgeting for training, technology investments, audits, and other related expenses.

This can be demonstrated through various forms of documentation. Here are detailed examples of documentation that can serve as evidence of resource allocation:

Resource Allocation Plan: An organization can create a formal resource allocation plan that outlines how resources will be distributed and managed for the ISMS. This plan can detail budget allocation, personnel assignments, and infrastructure upgrades. It serves as a clear roadmap for resource utilization :

<table>
<tr><td colspan="4">Organization: [Organization Name]</td></tr>
<tr><td>Objective</td><td colspan="3">This plan outlines the allocation of resources required to establish, implement, maintain, and continually improve the ISMS in compliance with ISO 27001</td></tr>
<tr><td rowspan="6">Resource categories</td><td rowspan="2">Financial Resources</td><td colspan="2">- Training and Development: [$X,XXX]
- Security Tools and Software: [$X,XXX]
- Consultation Services: [$X,XXX]
- Audit and Compliance: [$X,XXX]</td></tr>
<tr><td colspan="2">Total ISMS Budget: [$XX,XXX]</td></tr>
<tr><td>Human Resources</td><td colspan="2">- [Name, Position]
- [Name, Position]</td></tr>
<tr><td>Training and Development</td><td colspan="2">- List of training programs and allocated budget</td></tr>
<tr><td rowspan="3">Technology Resources:</td><td>Hardware and Software</td><td>- Inventory of hardware and software to be used in the ISMS
- Budget allocation</td></tr>
<tr><td>Security Tools:</td><td>- List of security tools and technologies to be acquired
- Budget allocation for security tools</td></tr>
<tr><td></td><td>Network and Infrastructure</td><td>budget allocation for network and infrastructure</td></tr>
<tr><td>Approval</td><td colspan="3">- [Name or Relevant Authority]
- [Date]</td></tr>
</table>

Budget Documentation: Maintaining a detailed budget that specifies the financial resources allocated to the ISMS is essential. This document should show line items for training, technology investments, security tools, consulting services, and other expenses related to information security :

ISMS Budget Documentation		
Organization: [Organization Name]		
Objective: This budget outlines the allocation of financial resources for the establishment, implementation, maintenance, and continuous improvement of the ISMS in compliance with ISO 27001.		
Budget Period: [Start Date] to [End Date]		
Financial Resources:		
Budget Category	**Allocation**	**Details**
Training	[$X,XXX]	Training programs and certification for staff involved in ISMS
Security Tools and Software	[$X,XXX]	Acquisition and licensing of security tools and software
Consultation Services	[$X,XXX]	Consulting services for ISMS implementation and audit
Miscellaneous Expenses	[$X,XXX]	Other expenses related to ISMS (e.g., documentation tools, awareness programs)
Total ISMS Budget	[$XX,XXX]	Total budget allocation for ISMS activities
Monitoring and Review: - The budget will be monitored and reviewed periodically to ensure effective allocation and adherence to the ISMS plan. - Adjustments may be made based on changing circumstances and organizational needs.		
[Name or Relevant Authority]		

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

The organization must identify and define the specific competencies and qualifications that its personnel need to perform their roles and responsibilities in a manner that contributes to the organization's information security objectives. These competencies are typically related to information security practices, policies, procedures, and the specific requirements of the ISO 27001 standard.

Competent personnel are critical to the successful implementation and maintenance of an ISMS. They are responsible for ensuring that security policies and procedures are followed, that security controls are effectively implemented, and that information security risks are managed appropriately

An organization can prove its compliance with the ISO 27001 clause related to determining the necessary competence of individuals affecting its information security performance through various means. Here are several methods to demonstrate and provide evidence of compliance:

Training Records: Maintain comprehensive records of all employee training and development programs related to information security. This should include documentation of the courses attended, certification achieved, and dates of training. This demonstrates that the organization invests in enhancing employee competence :

Training Records

Employee Name: [Employee's Full Name]
Employee ID: [Employee ID or Badge Number]
Department: [Employee's Department]
Date of Training: [Date of Training]

Training Program: [Name of Training Program]
Training Provider: [Name of Training Provider]
Training Location: [Location of Training]
Training Duration: [Duration of Training (e.g., hours)

Training Objectives:
- Briefly list the objectives or topics covered in the training program.
- Example: "This training covered topics such as risk assessment, incident response, and data protection."

Training Methods:
- Describe the training methods used (e.g., lectures, practical exercises, online modules).
- Example: "The training consisted of lectures and hands-on exercises."

Training Results:
- Note the results or outcomes of the training.
- Example: "The employee passed the certification exam with a score of 95%."

Trainer's Name: [Name of Trainer]
Trainer's Credentials: [Trainer's Qualifications]

Training Date Completed: [Date of Training Completion]

Employee's Signature: [Employee's Signature]

Manager's Approval: [Manager's Signature]

Job Descriptions and Role Assignments: Keep clear and up-to-date job descriptions and role assignments that outline the responsibilities and competencies required for each position. This documentation should reflect the alignment of job roles with the organization's information security requirements :

Information Security Manager

Job Description:

- **Job Title**: Information Security Manager
- **Reports To**: Chief Information Officer (CIO)
- **Job Purpose**: The Information Security Manager is responsible for leading and managing the organization's information security program. This role involves establishing and maintaining the information security management system (ISMS) and ensuring the organization's compliance with ISO 27001 standards.

Key Responsibilities:

- Develop, implement, and maintain the ISMS in line with ISO 27001 requirements.
- Oversee risk assessments, vulnerability assessments, and security audits.
- Identify and assess information security risks and provide recommendations for risk treatment.
- Ensure the development and maintenance of information security policies, procedures, and guidelines.
- Manage security awareness and training programs for employees.
- Coordinate incident response and investigation activities in the event of a security breach.
- Collaborate with IT teams to enforce security controls and monitor security performance.
- Provide regular reports and updates to executive management regarding information security status.
- Stay up-to-date with the latest information security trends and technologies.

Network Security Administrator

Job Description:

- **Job Title**: Network Security Administrator
- **Reports To**: IT Manager
- **Job Purpose**: The Network Security Administrator is responsible for the design, implementation, and maintenance of network security measures to protect the organization's information assets.

Key Responsibilities:

- Design and implement network security policies and configurations.
- Monitor network traffic for anomalies and security breaches.
- Manage firewall rules, intrusion detection/prevention systems, and antivirus solutions.
- Investigate and respond to security incidents and vulnerabilities.
- Conduct regular security assessments and penetration tests.
- Maintain and update network security documentation and diagrams.
- Collaborate with IT teams to ensure the security of network infrastructure.

Data Privacy Officer

Job Description:

- **Job Title**: Data Privacy Officer
- **Reports To**: Legal Counsel
- **Job Purpose**: The Data Privacy Officer is responsible for ensuring the organization's compliance with data protection and privacy laws, including GDPR and other applicable regulations.

Key Responsibilities:

- Develop and implement data protection policies and procedures.
- Oversee data privacy impact assessments and data breach notifications.
- Serve as a point of contact for data protection authorities and data subjects.
- Conduct data protection training for employees.
- Maintain records of data processing activities.
- Collaborate with legal and compliance teams on data privacy issues.

Skills Assessments: Conduct regular skills assessments or competency tests for individuals in key information security roles. The results of these assessments can serve as proof of the competence of personnel :

Example :

Employee Name: [Employee's Name] *Date of Assessment:* [Date]

Instructions: Please answer the following questions to the best of your ability. Rate your proficiency in each area on a scale of 1 to 5, with 1 being the lowest and 5 being the highest level of competency.

1. **Information Security Fundamentals**
   - Understanding of basic information security concepts: [Rating: 1-5]
   - Knowledge of the CIA (Confidentiality, Integrity, Availability) triad: [Rating: 1-5]
   - Familiarity with common security threats (e.g., malware, phishing): [Rating: 1-5]
2. **ISO 27001 Standards**
   - Understanding of ISO 27001 and its requirements: [Rating: 1-5]
   - Knowledge of ISO 27001 controls and their implementation: [Rating: 1-5]
3. **Risk Management**
   - Ability to identify and assess information security risks: [Rating: 1-5]
   - Proficiency in developing risk treatment plans: [Rating: 1-5]
4. **Access Control**
   - Knowledge of access control principles and techniques: [Rating: 1-5]
   - Competency in managing user access and permissions: [Rating: 1-5]
5. **Incident Response**
   - Ability to respond to security incidents effectively: [Rating: 1-5]
   - Familiarity with incident handling procedures: [Rating: 1-5]
6. **Security Awareness and Training**
   - Understanding of the importance of security awareness: [Rating: 1-5]
   - Proficiency in conducting security awareness and training programs: [Rating: 1-5]
7. **Security Policies and Procedures**
   - Knowledge of organization's security policies and procedures: [Rating: 1-5]
   - Ability to implement and enforce security policies: [Rating: 1-5]
8. **Data Encryption**
   - Understanding of data encryption principles: [Rating: 1-5]
   - Proficiency in implementing encryption for sensitive data: [Rating: 1-5]
9. **Network Security**
   - Knowledge of network security best practices: [Rating: 1-5]
   - Ability to configure and maintain network security controls: [Rating: 1-5]
10. **Security Tools and Technologies**
    - Familiarity with security tools (e.g., firewalls, antivirus): [Rating: 1-5]
    - Proficiency in using security technologies to monitor and protect systems: [Rating: 1-5]

Assessment Score: [Calculate the total score based on the individual's responses.]

Reviewer's Signature: [Signature of the person conducting the assessment]

Certifications: Maintain records of certifications and qualifications achieved by employees, particularly those related to information security. Certificates and qualifications serve as tangible evidence of a person's competence in specific areas

Example :

Employee Certifications and Qualifications		
Organization: [Organization Name]		
Employee Name: [Employee's Full Name]		
Position/Role: [Employee's Position or Role]		
List of Certifications and Qualifications:		
Certification/Qualification	**Issuing Body**	**Date Achieved**
ISO 27001 Lead	[Certification Body]	[Date Achieved]
Certified Information Security	[Certification Body]	[Date Achieved]
CISSP	[Certification Body]	[Date Achieved]
Monitoring and Review: - This document will be periodically reviewed and updated to ensure the accurate recording of employee certifications and qualifications.		
Responsibility: [Name of the Personnel Responsible for Document Management]		

Performance Reviews: Use performance reviews and evaluations to assess how well employees are meeting information security-related expectations and competencies. Documented reviews can provide evidence of employee competence.

Example :

Employee Details:

- **Name:** [Employee Name]
- **Position:** [Employee's Position]
- **Review Period:** [e.g., Annual Review - January 1, 2023, to December 31, 2023]

Reviewer Details:

- **Name:** [Reviewer's Name]
- **Position:** [Reviewer's Position]

I. Job Responsibilities and Objectives:

- **Job Description:** [Include a brief description of the employee's primary information security responsibilities and duties as outlined in their job description.]
- **Key Objectives:** [List the specific information security objectives and targets set for the employee during the review period.]

II. Competence and Skills Assessment:

Please rate the employee's performance on the following competencies and skills on a scale from 1 to 5 (1 = Unsatisfactory, 5 = Outstanding).

1. **Information Security Knowledge:** [ ] (1-5)
    - Demonstrates an understanding of information security principles, policies, and standards.
2. **Risk Management:** [ ] (1-5)
    - Effectively identifies, assesses, and mitigates information security risks.
3. **Compliance:** [ ] (1-5)
    - Adheres to information security policies, procedures, and regulatory requirements.
4. **Incident Handling:** [ ] (1-5)
    - Demonstrates effective incident response and resolution skills.
5. **Security Awareness:** [ ] (1-5)
    - Promotes security awareness and training among colleagues.

III. Accomplishments:

List the employee's major accomplishments and contributions in the area of information security during the review period.

- [Accomplishment 1]
- [Accomplishment 2]
- [Accomplishment 3]

IV. Areas for Improvement:

Identify any areas where the employee can improve their performance or competence in information security.

- [Area for Improvement 1]
- [Area for Improvement 2]

V. Overall Performance Rating:

Please provide an overall performance rating for the employee's information security-related work during the review period.

- **Overall Performance Rating:** [ ] (1-5)

Reviewer's Signature: _____Date: [Review Date]

Continual Improvement Records: Documentation showing how the organization identifies areas for improvement in employee competence and the actions taken to address these areas is another way to demonstrate compliance.

Example :

Continual Improvement Records		
Organization: [Organization Name]		
Objective: These records document the organization's efforts to continually improve employee competence in information security.		
Area of Improvement: Employee Competence in Information Security		
001	[Date]	Improvement Initiative Identified a knowledge gap in information security practices during an internal audit.
002	[Date]	Employee feedback indicated the need for advanced training on security incident response.
003	[Date]	During a skills assessment, it was observed that certain staff members lacked expertise in access control principles.
004	[Date]	A gap analysis of the workforce showed a need for enhanced understanding of ISO 27001 requirements.
005	[Date]	Employee self-assessments revealed a desire for more advanced cybersecurity training.

Action Taken:		
001	[Date]	Developed a customized training program to address the knowledge gap identified during the audit.
002	[Date]	Scheduled advanced training in security incident response based on employee feedback.
003	[Date]	Implemented an access control training program for staff members lacking expertise.
004	[Date]	Launched an ISO 27001 training program tailored to the workforce to address the gap analysis.
005	[Date]	Arranged advanced cybersecurity training courses to meet employee self-assessment needs.

Monitoring and Review:

- Regularly assess the impact of the improvement initiatives on employee competence in information security.
- Track participation, performance, and feedback from training and development programs.
- Make adjustments to initiatives as needed to ensure they are effective in improving competence.

Responsibility:

[Name of Responsible Party]

Training Plans: Maintain training plans that outline the training needs, schedules, and resources allocated to improving employee competence. These plans should align with the organization's information security objectives.

Example :

Information Security Training Plan	
Organization: [Organization Name]	
Objective: This training plan outlines the organization's commitment to enhancing employee competence in information security through structured training | and development programs.	
Training Period: [Start Date] to [End Date]	
Training Needs:	
Employee Category	**Training Needs and Objectives**
IT Staff	- Strengthen understanding of ISO 27001 - Improve incident response capabilities - Enhance knowledge of data protection laws - Master network security and firewall management
Non-Technical Staff	- Raise awareness of information security - Understand phishing and social engineering risks - Knowledge of password security and best practices

Managers	- Learn how to set information security policies and objectives - Improve risk management skills - Enhance the ability to lead and support security initiatives

Training Schedule:

- Training programs will be scheduled throughout the training period, taking into account the availability and job roles of employees. Training sessions will be conducted both in-house and through external providers.

Training Resources:

- Budget allocation for training programs: [$X,XXX]
- Internal trainers for in-house sessions
- Access to external training providers and their course offerings
- Training materials and resources (e.g., textbooks, online courses, simulations)
- Facilities for training sessions (e.g., meeting rooms, training equipment)

Monitoring and Review:

- Training effectiveness will be evaluated through post-training assessments and employee feedback. Adjustments to the training plan will be made based on results and changing needs.

Responsibility:

[Name of the Responsible Person or Department]

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy

b) their contribution to the effectiveness of the information security management system

c) the implications of not conforming with the information security management system requirements

The employees and relevant parties shall be aware of information security requirements. Here are the actions an organization should take:

Create an Information Security Awareness Program: Develop and implement an information security awareness program. This program should include activities, training, and communication efforts to ensure that all employees and relevant parties understand their roles and responsibilities in maintaining information security.

Example:

1. Introduction

- **Program Objectives**: Define the objectives of the awareness program, such as promoting a culture of security, reducing risks, and ensuring compliance with ISO 27001.
- **Program Scope**: Clearly state the scope of the program, including the roles and departments it covers.

2. Program Leadership and Responsibilities

- **Program Manager**: Appoint a program manager responsible for overseeing the program's development and implementation.
- **Responsibilities**: Outline the responsibilities of key individuals involved in the program.

3. Policy and Procedure Awareness

- **Information Security Policy**: Explain the organization's information security policy, its importance, and how employees can access it.
- **Security Procedures**: Provide an overview of key security procedures, such as password management, data classification, and incident reporting.

4. Training and Education

- **Security Training**: Identify mandatory security training programs and requirements for different job roles.
- **Training Content**: Specify the content of training modules, including data protection, malware prevention, and social engineering awareness.
- **Training Methods**: Describe the methods of training delivery, such as e-learning, workshops, or in-person sessions.
- **Frequency**: Indicate how often training should be conducted or refreshed.

5. Communication and Promotion

- **Awareness Campaigns**: Plan and execute awareness campaigns using various channels, such as emails, posters, and the organization's intranet.
- **Incident Reporting**: Highlight the importance of reporting security incidents promptly and provide guidance on how to do so.
- **Feedback Mechanism**: Establish a feedback mechanism for employees to report security concerns or suggest improvements.

6. Role-Based Training

- **Customized Training**: Tailor training to specific job roles, emphasizing the unique security responsibilities of each role.
- **Management Training**: Include training for managers on their role in promoting information security within their teams.

7. Monitoring and Metrics

- **Awareness Metrics**: Define key performance indicators (KPIs) for measuring awareness, such as training completion rates.
- **Feedback Surveys**: Conduct surveys to gather feedback on the effectiveness of the program and identify areas for improvement.

8. Compliance Checks

- **Audit and Compliance Checks**: Specify how and when compliance checks and audits will be conducted to ensure adherence to security policies and procedures.
- **Consequences for Non-Compliance**: Communicate the consequences for non-compliance, such as disciplinary actions.

9. Documentation

- **Documentation Retention**: Define the process for retaining records of training, awareness activities, and incident reports.
- **Incident Logs**: Maintain logs of security incidents and their resolution.

10. Continuous Improvement

- **Continuous Evaluation**: Regularly assess the effectiveness of the program and make adjustments as necessary.
- **Program Enhancements**: Document how feedback from employees and changing threats are used to improve the program.

11. Legal and Regulatory Compliance

- **Data Protection Laws**: Highlight the organization's commitment to complying with data protection laws and regulations.
- **Legal Requirements**: Ensure that employees are aware of their obligations under relevant legal and regulatory requirements.

12. Management Support

- **Executive Support**: Emphasize the active support and involvement of top management in promoting information security awareness.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the processes by which communication shall be effected

Refers to the requirement for an organization to assess and identify its communication needs concerning its Information Security Management System (ISMS). This clause underscores the importance of establishing effective communication mechanisms both within the organization (internal) and with external parties when it comes to information security.

Information Security Communication Plan

Communication Type	Audience	Purpose	Method/Channel	Frequency/Trigger	Responsible Person	Documentation
Internal Communication						
Information Security Policy	All Employees	Raise awareness and gain commitment	Email, Intranet, Meetings	Annually, New Policy Adoption	Information Security Officer	Policy Orientation Records
Incident Reporting Guidelines	All Employees	Educate employees on reporting process	Training Sessions	Annually, New Employee Training	Information Security Officer	Training Records
External Communication						
Data Breach Notification	Affected Customers	Notify customers of data breach	Email, Letter, Phone	As Needed, Data Breach Occurs	Communications Manager	Breach Notification Letters
Regulatory Authorities	Relevant Authorities	Report data breaches to regulators	Official Reporting Channels	As Required, Data Breach Occurs	Legal Department	Regulatory Reports
Vendor Security Expectations	Third-Party Vendors	Communicate security requirements	Vendor Contracts	During Contract Negotiations	Procurement Department	Vendor Contracts
Vendor Security Updates	Third-Party Vendors	Communicate security updates	Email, Vendor Portal	Annually, Ongoing Monitoring	Procurement Department	Vendor Correspondence

Identifying the Need for Internal Communication:

1. **Information Security Policy Adoption**: The organization's leadership has developed a comprehensive Information Security Policy as part of the ISMS implementation. The need for internal communication arises when the organization wants to ensure that all employees are aware of the policy's existence, understand its importance, and know how to access it. The objective is to gain their commitment to adhering to the policy.
    - **Action**: The organization plans an internal communication campaign. It sends out a company-wide email announcing the new policy, highlighting its significance, and providing a link to the full document. The communication also encourages employees to attend a mandatory policy orientation session, which will be organized in various departments.
2. **Security Incident Reporting**: To bolster the organization's ability to respond to security incidents, it establishes a clear incident reporting procedure. All employees should be aware of how to report security incidents promptly to the designated security team.
    - **Action**: The organization includes incident reporting guidelines in its employee handbook and conducts mandatory training sessions that explain the reporting process. They ensure that all employees are aware of the dedicated email address and phone number for reporting incidents, as well as the internal escalation process.

Identifying the Need for External Communication:

1. **Data Breach Reporting**: The organization recognizes that, in the event of a data breach involving customer data, it has a legal and ethical responsibility to communicate this breach to affected customers and potentially regulatory authorities.
    - **Action**: The organization establishes a data breach response plan that includes communication procedures. It outlines who within the organization is responsible for notifying customers, regulatory bodies, and the public, if necessary. This plan includes templates for breach notification letters to affected customers, providing details about the breach and steps the organization is taking to mitigate the impact.
2. **Third-Party Vendors**: The organization works with several third-party vendors who have access to its systems and data. It acknowledges that communicating information security expectations and requirements to these vendors is essential to ensure they comply with the organization's security standards.
    - **Action**: The organization establishes a clear communication process with vendors. It develops a vendor security policy, requiring vendors to sign agreements that specify their security responsibilities. The policy is communicated to vendors during contract negotiations and reviewed periodically.

Internal Communication Procedure

Purpose: To ensure that all employees are informed about relevant information security matters.

What to Communicate:

1. Information Security Policy: To inform employees of the organization's commitment to information security.
2. Security Incidents: To communicate the occurrence and resolution of security incidents.
3. Training Programs: To announce upcoming training sessions.
4. Security Updates: To share information about new threats and preventive measures.

When to Communicate:

1. Information Security Policy: Annually or upon policy updates.
2. Security Incidents: As soon as possible after incident detection and resolution.
3. Training Programs: Before the start of each training session.
4. Security Updates: Regularly as new threats emerge.

With Whom to Communicate:

1. Information Security Policy: All employees.
2. Security Incidents: Incident Response Team, relevant employees, and affected parties.
3. Training Programs: Employees scheduled for training.
4. Security Updates: All employees.

Who Shall Communicate:

1. Information Security Policy: Information Security Officer.
2. Security Incidents: Incident Response Team lead.
3. Training Programs: HR or Training Coordinator.
4. Security Updates: Information Security Officer or designated security personnel.

Processes by Which Communication Shall Be Effected:

1. Information Security Policy:
    - The Information Security Officer shall send an email to all employees, attaching the updated policy document and providing a summary of the changes.
    - The policy shall also be posted on the company intranet.
2. Security Incidents:
    - The Incident Response Team lead shall inform relevant employees immediately through email and phone calls.
    - A detailed incident report shall be distributed to affected parties and regulatory authorities as necessary.

3. Training Programs:
    - The HR or Training Coordinator shall send email invitations to employees scheduled for training, including training dates, times, and locations.
    - Employees shall also receive calendar invitations.
4. Security Updates:
    - The Information Security Officer or designated personnel shall send periodic security update emails with relevant information and best practices.
    - Security posters and notices shall be posted on noticeboards.

External Communication Procedure

Purpose: To effectively communicate information security matters with external parties, including customers, suppliers, regulatory authorities, and third-party vendors.

What to Communicate:

1. Data Breach Notifications: To inform affected customers about data breaches.
2. Compliance Reports: To report information security compliance to regulatory authorities.
3. Vendor Security Expectations: To communicate security expectations to third-party vendors.
4. Security Updates to Third-Party Vendors: To provide updates on security requirements.

When to Communicate:

1. Data Breach Notifications: As soon as possible after identifying a data breach.
2. Compliance Reports: According to regulatory deadlines.
3. Vendor Security Expectations: During contract negotiations.
4. Security Updates to Third-Party Vendors: Annually or as needed.

With Whom to Communicate:

1. Data Breach Notifications: Affected customers.
2. Compliance Reports: Relevant regulatory authorities.
3. Vendor Security Expectations: Third-party vendors.
4. Security Updates to Third-Party Vendors: Third-party vendors.

Who Shall Communicate:

1. Data Breach Notifications: Communications Manager.
2. Compliance Reports: Legal Department.
3. Vendor Security Expectations: Procurement Department.
4. Security Updates to Third-Party Vendors: Procurement Department.

Processes by Which Communication Shall Be Effected:

1. Data Breach Notifications:
    - The Communications Manager shall send notifications to affected customers via email, postal mail, and phone calls as necessary.
    - A copy of the notification shall be provided to the Legal Department for regulatory reporting.
2. Compliance Reports:
    - The Legal Department shall submit compliance reports through official regulatory channels as required.
3. Vendor Security Expectations:

- During contract negotiations, the Procurement Department shall communicate security expectations and requirements to third-party vendors.
- Vendor agreements shall include security clauses.

4. Security Updates to Third-Party Vendors:
    - Annually, the Procurement Department shall send security updates to third-party vendors via email or through a designated vendor portal.

7.5 Documented information

The organization’s information security management system shall include:

a) documented information required by this International Standard; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system

An organization's Information Security Management System (ISMS) must encompass two categories of documented information:

a) **Documented Information Required by ISO 27001**: This category encompasses the specific documentation that is explicitly mandated by the ISO 27001 standard itself. This includes documents such as:

- The Information Security Policy: A documented statement of an organization's commitment to information security.
- Risk Assessment and Treatment Methodology: The methodology for identifying, assessing, and treating information security risks.
- Statement of Applicability (SoA): A document specifying which controls from Annex A of ISO 27001 are applicable and the justification for their inclusion or exclusion.
- Records of Monitoring and Measurement Results: Records of the results from monitoring and measurement activities related to information security performance.
- Internal Audit Reports: Documentation of the findings and results of internal audits.
- Non-conformity and Corrective Action Records: Records of non-conformities, corrective actions taken, and their effectiveness.

These documents are explicitly required by ISO 27001 and must be established and maintained to comply with the standard.

b) Documented Information Determined by the Organization: In addition to the documents explicitly required by ISO 27001, the organization has the flexibility to identify and define other documents that it deems necessary for the effective operation of its ISMS. These documents are organization-specific and may include:

1. **Customized ISMS Manual**: A manual that provides a detailed description of the organization's ISMS structure, including its policies, procedures, responsibilities, objectives, and organization-specific performance indicators.
2. **Information Asset Inventory**: A comprehensive list of the organization's information assets, including their value, ownership, classification, associated threats, and implemented security measures.

3. **Organization-Specific Risk Matrix**: A detailed risk matrix that identifies organization-specific threats, vulnerabilities, consequences, and associated mitigation measures.
4. **Corrective and Preventive Action (CAPA) Plans**: Documentation of specific actions taken by the organization to address non-conformities, security incidents, or to prevent future issues.
5. **Specific Operational Procedures**: Detailed procedures that describe how certain information security-related activities or processes are conducted within the organization. For example, procedures for access management, password management, or system monitoring.
6. **Supplier Management Policy**: An organization-specific policy that outlines information security requirements for suppliers and third parties with which the organization conducts business.
7. **Security Incident Management Procedure**: A detailed procedure that describes how the organization manages security incidents, including notification, investigation, response, and corrective actions.
8. **Change Management Procedure**: An organization-specific procedure that outlines how changes to systems, processes, or infrastructure are assessed, authorized, tested, and implemented while considering information security.
9. **Training and Awareness Record**: A record that tracks information security training and awareness sessions provided to employees, including dates, participants, and topics covered.
10. **Regulatory Compliance Documentation**: Any organization-specific documentation that demonstrates compliance with information security laws and regulations, such as certifications or audit reports.

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

a) **Identification and Description**:

For example, a document should have a descriptive title, the date it was created or last updated, the name of the author or responsible party, and a reference number or version identifier. This information ensures that the document can be easily recognized, tracked, and controlled.

b) **Format and Media**:

- For example, if a document is available in multiple languages, it should be clearly indicated. The use of specific software versions ensures compatibility and consistency. Graphics and visuals can be used to enhance understanding.
- The choice of media (e.g., paper or electronic) should be appropriate for the document's purpose and accessibility.

c) **Review and Approval for Suitability and Adequacy**:

- Before a document is finalized or updated, it should go through a review and approval process to ensure its suitability and adequacy for the intended purpose. This process typically involves relevant personnel or stakeholders.
- The review and approval process helps confirm that the document accurately represents the organization's policies, procedures, or other documented information. It ensures that the document aligns with the organization's goals and meets any legal, regulatory, or standard requirements.

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and f) retention and disposition.

Here are the key steps and considerations for controlling documented information within the ISMS:

1. **Identification and Classification**:
    - Begin by identifying the various types of documented information required by the ISMS, such as policies, procedures, records, and reports.
    - Classify these documents based on their criticality, sensitivity, and relevance to information security.
2. **Access Control**:
    - Control access to documented information by defining who can access, modify, and approve it. Access should be based on roles and responsibilities.
    - Implement strong access controls to prevent unauthorized access and ensure that only authorized personnel can view or edit the documents.
3. **Version Control**:
    - Maintain a version control system to manage document revisions. This helps ensure that the latest version is available and used.
    - Clearly label and track document versions, and establish procedures for updating and distributing new versions.
4. **Distribution and Availability**:
    - Establish distribution procedures to ensure that documented information is available to relevant personnel when and where it is needed.
    - Provide access through electronic systems, intranets, or document repositories to make information readily available.
5. **Backup and Recovery**:
    - Implement backup and recovery procedures for critical documented information to safeguard against data loss or corruption.
    - Regularly back up electronic documents and store them in secure and accessible locations.

6. **Review and Approval**:

- Documents should undergo a review and approval process to ensure they are suitable and up to date.
- Define responsibilities for reviewing and approving documented information, and establish review cycles.

7. **Change Management**:

- Changes to documented information should be managed through a formal change control process.
- Ensure that changes are reviewed, approved, and communicated to relevant parties, and that previous versions are archived.

8. **Retention and Disposal**:

- Define retention periods for various types of documented information. Retain documents for the necessary duration to meet legal and regulatory requirements.
- Implement secure disposal procedures for documents that have reached the end of their retention period.

8 - Operation

8.1 Operational planning and control

The organization shall implement the actions determined in 6.1.

- The organization shall also implement plans to achieve information security objectives determined in 6.2.

- The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

1. **Implementing Actions Determined in 6.1**

- Clause 6.1 (organization determining actions to address risks and opportunities).

- Putting in place the necessary controls, policies, procedures

Access Control Team

- Appoint an Access Control Team responsible for implementing access control measures.
- This team should include IT administrators, security personnel, and relevant stakeholders.

Define Access Control Policy:

- Develop an Access Control Policy that outlines the guidelines for controlling access to information assets.
- This policy will set the foundation for access control measures.

Access Control Matrix

Create an Access Control Matrix that lists all information assets, classifies them by sensitivity (e.g., public, confidential, secret), and specifies the level of access required for each asset.

User Access Classification

- Classify users and roles based on their job functions and access requirements.

- For example, employees may be categorized into standard users, privileged users, and administrators.

Access Control Software:

- Implement access control software that allow management of user accounts, roles, permissions, and authentication methods.
- This may include solutions like identity and access management (IAM) systems.

User Authentication:

- Enforce strong user authentication methods such as two-factor authentication (2FA) for sensitive systems or data. Users may be required to use a combination of passwords and authentication tokens.

User Account Management:

- Establish procedures for creating, modifying, and deactivating user accounts. This includes defining the process for onboarding new employees and disabling access for departing employees.

User Training:

- Provide user training and awareness programs to educate employees about access control policies and best practices. Users should understand the importance of protecting their credentials.

Monitoring and Logging:

- Implement monitoring and logging systems to track access and user activities.
- Monitor for suspicious activities and unauthorized access attempts.

2. Implementing Plans to Achieve Information Security Objectives Determined in 6.2:

- Implementation of information security objectives

- These objectives involves creating action plans to achieve them. These plans specify the tasks, responsibilities, timelines, and resources.
- By implementing these plans, the organization works toward improving its information security posture.

Risk Assessment:

- The organization conducts a risk assessment to identify potential security risks related to user awareness. This includes the risk of employees falling victim to phishing attacks or not following security policies.

Objective Definition:

- The organization sets a specific objective to enhance user awareness training on information security.
- Ex: Achieve a 98% success rate in user awareness training on information security within the next year (This means that 98% of employees should successfully complete the training)

Action Plan Development:

- **Content Development**: develops training content, including videos, quizzes, and informational resources.
- **Training Schedule**: Create a training schedule that ensures all employees receive training within the year.
- **Training Delivery**: Implement a learning management system (LMS) to deliver the training, track progress, and provide certificates upon completion.
- **Assessment and Feedback**: Include assessment quizzes and a feedback mechanism to assess the effectiveness of the training and gather employee feedback.

- Reminder Campaigns: Send periodic reminders to employees to complete the training.

Action Plan Development:

- **Responsibility Assignment**: Designate a training coordinator and assign responsibility to relevant departments for creating content, scheduling training sessions, and managing the LMS.

Action Plan Development:

- - **Resource Allocation**: Allocate budget and resources to support the action plan, including LMS software, content development, and personnel for training coordination.
- **Timelines**: Establish a timeline for each action item, such as launching the LMS within three months, starting training within six months, and completing the training within a year.
- **Monitoring and Measurement**: Use the LMS to monitor and measure employee progress and completion rates. Analyze the quiz results and feedback to assess the effectiveness of the training content.

3. Keeping Documented Information for Process Verification:

- The organization must keep records and evidence of the activities related to the ISMS.
- These records serve as proof that the organization has carried out its information security activities and procedures as planned and in compliance with ISO 27001 requirements

Records of Activities: document the execution of specific actions. They may include activities such as:

incident

access control

training and awareness

Evidence of Compliance: provide evidence that the organization is complying with the requirements and controls specified in ISO 27001.

For example, evidence of :

regular security audits

risk assessments

corrective actions

Example:

- **Incident reports:** Incident logs, response procedures, and post-incident reviews
- **Access control :** Access control policies, access request forms, and access logs
- **Training and Awareness:** Training schedules, training materials, and participant sign-in sheets
- **Security Audits:** Audit reports, audit schedules, and evidence of corrective actions taken
- **Data Backup and Recovery:** Backup and recovery plans, logs of backup activities, and test results

- The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur.
- The organization shall retain documented information of the results of the information security risk assessments

- The organization must determine planned intervals for conducting the risk assessments.
- The specific frequency of risk assessments can vary based on factors such as the organization's size, the rate of change in the information environment, and the level of risk exposure
- Document the results of risk assessments, including the identified risks, their assessments, and the risk treatment plans
- organizations should implement continuous monitoring processes to detect and respond to emerging risks and changes in the risk landscape between planned assessments
- Risks that the organization chooses to accept, rather than mitigate, should be clearly documented and communicated to relevant stakeholders

Audit Schedule for Information Security Risk Assessments

Audit/Assessment Type	Interval	Responsible	Planned Audit Date
Annual Risk Assessment	Annually	Team X	[Date]
Quarterly IT Security Audit	Quarterly	Auditor Y	[Date]
Third-Party Vendor Audit	Semi-Annually	Vendor Mgmt	[Date]
Application Security Review	Bi-Annually	Security Team	[Date]
Compliance Audit (ISO 27001)	Annually	Internal Audit	[Date]
Incident Response Drill	Monthly	Incident Team	[Date]

Audit Schedule for Major Change-Triggered Audits and Assessments

Audit/Assessment Type	Triggering Change Type	Responsible	Audit Date
Post-System Upgrade Audit	Major IT System Upgrade	IT Team	[Date]
Data Migration Assessment	Data Migration Project	Data Team	[Date]
Compliance Audit (Regulatory)	New Data Privacy Law	Compliance Team	[Date]
Vendor Security Review	Change in Vendor	Vendor Mgmt	[Date]
Security Incident Review	Major Security Incident	Incident Team	[Date]

Risk Assessment Report

Document Control Information:

- Document Title: Risk Assessment Report
- Document Reference Number: RA-2023-001
- Date of Issue: October 15, 2023
- Version: 1.0
- Prepared by: John
- Approved by: Jane

Risk Treatment Prioritization :
The risk treatment plans have been prioritized based on risk levels, with a focus on addressing high-risk items first.

Monitoring and Review :
The progress of risk treatment will be continuously monitored, and quarterly reviews will be conducted to track progress and make necessary adjustments.

Conclusion :
This Risk Assessment Report highlights the significance of ongoing risk management and the organization's commitment to safeguarding information security.

Document Revision :
This Risk Assessment Report will be reviewed and updated as necessary to reflect changes in the risk landscape.

Approval :
This Risk Assessment Report is approved by Jane Doe, Chief Information Security Officer, on October 15, 2023.

- The organization shall implement the information security risk treatment plan
- The organization shall retain documented information of the results of the information security risk treatment

- This means putting into action the measures identified in the risk treatment plan
- The risk treatment plan is a document that outlines how the organization intends to manage and mitigate information security risks
- It should cover a systematic approach to identifying, assessing, treating risks:

Risk ID	Risk description	likelihood	Impact	Treatement Impact
R001	Unauthorized access to sensitive data	Medium	High	- Implement stricter access controls - Implement MFA for sensitive systems - Conduct access audits
R002	Malware infection on workstations	Low	Medium	- Deploy antivirus software on workstations - Conduct employee training on malware prevention

- **Documented Information:** This refers to records, reports, or any form of documentation that provides evidence of the activities and results related to the information security risk treatment.
- This information may include:

  risk assessments,

  treatment plans,

  incident reports

9 - Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

a) what needs to be monitored and measured

b) the methods for monitoring, measurement, analysis and evaluation,
c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure

e) when the results from monitoring and measurement shall be analyzed and evaluated

f) who shall analyze and evaluate these results

Evaluating the effectiveness of information security processes and controls

- Processes and controls are defined in 6.1
- key performance indicators (KPIs) are defined in 6.2 (align with the organization's information security objectives)
- KPI = for each process and control we must define performance metrics.
- These KPI should be quantifiable and specific (For example, average time to resolve security incidents)

Example 1 :

Risk Title: Malware Infection Risk

Risk Description: Potential of malware infections that can be introduced through various vectors, such as malicious email attachments, infected software downloads

Risk Impact: (Financial Costs): Remediation and recovery from virus infections can result in financial expenses for the organization

Risk Treatment Measures: Antivirus Software, Email Filtering, User Training

Objective: Reduce the risk of malware infections, including viruses, to an acceptable level

KPI 1 = 98% of endpoints with up-to-date antivirus signatures (within 2 months)

KPI 2 = 1% of employees who click on phishing emails (within 3 months)

Monitoring:

> **Endpoint Scanning**: Regularly schedule scans of all endpoints (computers and devices) to check for the presence and status of antivirus signatures (detect number of endpoints with outdated antivirus signatures)

Reporting:

Monthly Reports: Generate monthly reports summarizing the percentage of endpoints with up-to-date antivirus signatures. Include any deviations from the 98% target.

How to Monitor Incidents

Parameter	Description
a) What Needs to Be Monitored and Measured	**Incidents:** All security incidents, including but not limited to data breaches, malware infections, system intrusions, and unauthorized access attempts.
b) Methods for Monitoring, Measurement, Analysis, and Evaluation	- **Monitoring:** Real-time monitoring of security events and alerts generated by security systems. - **Measurement:** Tracking and recording the details of security incidents in an incident management system. This includes the incident type, date of detection, and resolution time. - **Analysis and Evaluation**: Regular review and analysis of incident data to determine if they were detected within the defined timeframe.
c) When the Monitoring and Measuring Shall Be Performed	- **Monitoring:** Ongoing, 24/7 real-time monitoring of security events. - **Measurement:** Incidents are logged and recorded immediately upon detection. - **Analysis and Evaluation:** Periodic reviews are conducted on a quarterly basis.
d) Who Shall Monitor and Measure	- **Monitoring and detection** are performed by the IT Security and Incident Response Team. - **Incident details** are logged and maintained by the IT Security Team. - **Analysis and evaluation** are conducted by the Chief Information Security Officer (CISO) and the Incident Response Team.
e) When the Results from Monitoring and Measurement Shall Be Analyzed and Evaluated	- **Analysis and evaluation** occur on a quarterly basis, with the first analysis to be completed at the end of the first quarter.
f) Who Shall Analyze and Evaluate These Results	- **The Chief Information Security Officer (CISO)** will lead the analysis and evaluation process, with support from the Incident Response Team for incident-specific assessments.

Month	Number of Incidents Detected	Total Incidents	Percentage Detected	Incident Type	Date of Detection	Resolution Time
Month 1	15	20	75%	Malware Infection	[Date]	[Time]
Month 2	18	22	82%	Malware Infection	[Date]	[Time]
Month 3	20	23	87%	Malware Infection	[Date]	[Time]

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to:

1) the organization’s own requirements for its information security management system; and

2) the requirements of this International Standard;

b) is effectively implemented and maintained.

1. **Internal Audits:**

   The organization is responsible for conducting regular internal audits of its ISMS

2. **Conformity to Own Requirements:**

   The primary purpose of these internal audits is to: determine whether the ISMS aligns with the organization's own requirements. This includes assessing whether the ISMS meets the organization's:

   policies

   procedures

   objectives

3. **Independence and Objectivity:**

   The internal audits should be carried out by individuals or teams that are independent and objective. This means that auditors should not audit their own work

Example:

Data and Record Examination:

Analyze Logs and Records: The auditor examines logs and records related to antivirus activities, including software installation, updates, scanning, and malware detection.

Endpoint Inspection:

Physical Inspection: The auditor may physically inspect a sample of endpoint devices to verify the presence of antivirus software, check for up-to-date virus definition databases, and assess the regularity of malware scans.

Performance Against KPI:

Check Compliance with KPI: If a KPI related to antivirus compliance is in place, the auditor checks whether the organization is meeting the KPI's target. Non-compliance with the KPI may indicate non-conformities.

Evidence of Non-Conformity:

- Several endpoint devices within the organization have outdated antivirus software
- some have not received virus definition updates for a significant period.
- Scanning logs reveal that some devices have not been regularly scanned as required by the policy and procedure

- There is no documented evidence of deviations being reported.

Recommandation

Corrective actions to address this non-conformity:

- Update antivirus software on all endpoint devices to the latest version.
- Establish a process for regular scanning and ensure it aligns with the policy.

- Report deviations

- Conduct training and awareness programs to emphasize the importance of compliance with the antivirus policy.

Audit Criteria: Clause 4 - Context of the Organization

It helps ensure that the organization has identified and considered external and internal factors that can affect its information security management system (ISMS)

1. Audit Objective:

To assess whether the organization has effectively considered its context, both internal and external, in relation to its ISMS.

2. Audit Planning:

Identify the key stakeholders to interview, such as top management, information security personnel, and risk management teams.

3. Review of Context Analysis:

- Obtain and review the organization's documented context analysis.

- Ensure that the analysis includes external issues (e.g., Political, Economic, legal and regulatory requirements, ….) and internal issues (e.g., organizational structure, culture, resources).

4. Top Management Commitment:

Interview top management to assess their understanding of the organization's context and its relevance to information security.

5. Identification of Interested Parties:

- Review the organization's identification of interested parties relevant to the ISMS, such as customers, regulators, and suppliers.

- Evaluate the organization's ability to identify and document internal and external issues that can affect its ISMS.

- Check if there are processes in place for monitoring and reviewing these issues.

6. Reporting of Audit Findings:

Document any non-conformities related to the organization's context analysis.

7. Audit Findings:

- The organization has conducted a context analysis, considering both internal and external factors, and has documented the findings.

- Top management demonstrates a clear understanding of the context and actively communicates the importance of information security within that context.

- Interested parties that can impact the ISMS have been identified and are regularly reviewed.

Audit Criteria: Clause 5 – Leadership

1. Audit Objective:

- Examine the organization's Information Security Policy to ensure it is documented, approved by top management, and communicated to all relevant parties.
- Verify that information security objectives are established and aligned with the organization's strategic goals.

2. Management Commitment:

Assess top management's commitment to information security by reviewing documented statements

3. Organizational Roles and Responsibilities:

- Review the organization's documented roles and responsibilities for information security.

- Ensure that there is a clear designation of roles responsible for information security within the organization.

4. Resource Allocation:

- Verify that resources, including personnel, budgets, and technology, are allocated to support the ISMS.
- Ensure top management communicates the importance of information security more effectively.

5. Evidence Gathering:

Collect evidence, including policy documents, organizational charts, responsibilities records, …..

Audit Criteria: Clause 6 – planning

Including risk assessment, risk treatment and objectives

1. Risk Assessment:

- Review the documented process for conducting a risk assessment.

- Evaluate the identification of information assets, threats, vulnerabilities, and the assessment of their potential impacts.

- Verify the methodology used for assessing risks.

- Assess how the organization determines the acceptable level of risk.

2. Risk Treatment:

- Examine the risk treatment plan and its alignment with the identified risks.

- Verify the measures and controls selected for risk mitigation.

- Check if residual risks are accepted, avoided, transferred, or mitigated.

- Ensure that risk treatment decisions are documented

3. Information Security Policy:

- Review the organization's Information Security Policy.

- Ensure that it is approved by top management and communicated to all relevant parties.

- Assess the alignment of the policy with the organization's context and objectives.

- Verify if the policy is available to interested parties.

4. Risk Treatment:

- Examine the risk treatment plan and its alignment with the identified risks.

- Verify the measures and controls selected for risk mitigation.

- Check if residual risks are accepted, avoided, transferred, or mitigated.

    - Ensure that risk treatment decisions are documented

5. Information Security Policy:

- Review the organization's Information Security Policy.

- Ensure that it is approved by top management and communicated to all relevant parties.

- Assess the alignment of the policy with the organization's context and objectives.

- Verify if the policy is available to interested parties.

6. Information Security Objectives:

- Review how information security objectives are established.

- Evaluate the documented objectives and their alignment with the Information Security Policy.

- Ensure that objectives are measurable and have defined timelines.

- Check if responsibilities for achieving objectives are assigned.

7. Corrective Actions:

- Adjusting policies, procedures, or controls to align with ISO 27001 requirements for Clause 6

(Ex: Policy did not provide clear guidance on the process of risk assessment and risk treatment, as required by ISO 27001 Clause 6.1, It did not define how risks should be identified, analyzed, and evaluated within the organization, did not specify the criteria for accepting, avoiding, transferring, or mitigating risks)

Audit Criteria: Clause 7 – support

1. Objective:

Assess the organization's conformity with ISO 27001 requirements related to support functions

2. Resource Allocation:

- Assess the allocation of resources to the ISMS, including personnel, technology, infrastructure, and financial resources

- Review budgetary allocations and resource planning documents

3. Competence and Training:

- Evaluate the competence of personnel involved in ISMS roles, such as information security managers

- Review training records and certifications to ensure that employees are adequately trained in information security

4. Awareness and Communication:

- Verify that there are awareness programs in place to educate employees about information security

- Assess how communication mechanisms ensure that information security requirements are effectively conveyed to all relevant parties.

5. Documented Information:

- Review the organization's documented information relevant to the ISMS, such as policies, procedures, and records

- Ensure that documented information is controlled, regularly updated, and accessible to those who need it

6. Audit Findings:

Identify non-conformities or areas where the organization does not meet ISO 27001 requirements. For example, non-conformities could include:

- Inadequate allocation of resources to the ISMS.

- Insufficient training and competence of personnel.

- Lack of awareness programs or ineffective communication.

- Poor control and maintenance of documented information.

Audit Criteria: Clause 8 – operation

8.1 - Operational planning and control:

1. Audit Objective:

To assess the organization's compliance with operational planning and control requirements

2. Audit Steps:

- Review the organization's operational plans related to information security.

- Verify that these plans align with the organization's risk assessment and risk treatment processes.

- Check for documented procedures for information security operations.

8.2 - Information security risk assessment:

1. **Audit Objective:**

To ensure that the organization's risk assessment processes are in line with ISO 27001 requirements.

2. Audit Steps:

- Review the organization's documented risk assessment methodology
- Evaluate the risk assessment process, including the identification, analysis, and evaluation of information security risks

- Check that risks are assessed with respect to confidentiality, integrity, and availability

Audit Criteria: Clause 9 – Performance evaluation

9.1 Monitoring, Measurement, Analysis, and Evaluation:

1. **Objective:**

- Assess the organization's conformity with ISO 27001 requirements related to monitoring, measurement, analysis, and evaluation of the ISMS

2. Audit Steps:

a. Monitoring and Measurement:

- Review documented procedures for monitoring and measurement of information security performance

- Verify that metrics and key performance indicators (KPIs) are defined and aligned with the ISMS objectives

b. Analysis and Evaluation:

- Assess the process of analyzing and evaluating the collected data

- Verify that there are processes to identify non-conformities and security incidents

c. Internal Audit :

- Assess the planning and execution of internal audits

d. Evidence Gathering:

- Collect evidence, including monitoring and measurement records, analysis reports, and records of non-conformities and incidents

e. Audit Findings:

- Identify non-conformities or areas where the organization does not meet ISO 27001 requirements for monitoring, measurement, analysis, and evaluation.

Audit Criteria: Clause 10 – Improvement

1. Objective:

Assess the organization's conformity with ISO 27001 requirements related to handling of non-conformities, corrective actions, and preventive actions

2. Audit Planning:

Identify the areas within the ISMS where improvement processes are applicable

3. Audit Preparation:

- Review Clause 10 of ISO 27001 to understand the requirements.

- Examine the organization's documented procedures for handling non-conformities, corrective actions, and preventive actions.

4. Non-Conformity Handling:

- Review records of identified non-conformities within the ISMS.

- Assess the process for identifying, documenting, and categorizing non-conformities.

- Check whether there are clearly defined responsibilities for non-conformity handling.

- Verify that non-conformities are investigated to determine their root causes.

5. Corrective Action Process:

- Examine records of corrective actions taken in response to non-conformities

- Assess the process for identifying and implementing corrective actions

- Verify that corrective actions address the root causes of non-conformities

- Check for documented evidence of the effectiveness of corrective actions

6. Preventive Action Process:

- Review records related to preventive actions within the ISMS.

- Assess the process for identifying and implementing preventive actions to address potential issues and risks.

- Verify that preventive actions are designed to prevent the occurrence of non-conformities.

- Check for documented evidence of the effectiveness of preventive actions.

The organization shall:

c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

d) define the audit criteria and scope for each audit;

e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) ensure that the results of the audits are reported to relevant management; and :

g) retain documented information as evidence of the audit programme(s) and the audit results

This audit program helps ensure that the organization's information security practices align with ISO 27001 requirements and are effective in safeguarding information assets

1. Audit Program Scope and Objectives:

- Define the scope of the audit program

- specifying which areas of the ISMS will be audited

- Establish clear objectives for the audit program (such as assessing compliance with ISO 27001 requirements, identifying non-conformities, and promoting continuous improvement)

2. Audit Program Planning:

- Develop a detailed plan that outlines the frequency, timing, and scheduling of audits. This plan can cover an annual audit cycle.

- Identify the auditors who will be responsible for conducting the audits.

- Determine the audit methodology and procedures to be followed.

3. Audit Program Implementation:

- Conduct the planned audits in accordance with the audit program.
- Auditors should follow established audit procedures and use checklists, to assess conformity with ISO 27001 requirements.

4. Audit Program Review and Adjustment:

- Regularly review the audit program to ensure it remains effective and aligned with organizational goals.

- Make adjustments to the audit program based on the findings and recommendations from previous audits.

5. Audit Reporting:

- Prepare audit reports after each audit, summarizing the findings, observations, non-conformities, and recommendations.

- Clearly communicate the results of the audits to relevant stakeholders.

10 - Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it; and

2) deal with the consequences

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

The organization shall retain documented information as evidence of:

e) the nature of the nonconformities and any subsequent actions taken, and

f) the results of any corrective action

1. objective

- it is essential for the organization to react promptly and effectively to address the nonconformity. This involves taking actions to control and correct the nonconformity, as well as dealing with the consequences that may result from it

2. Identify

- When a nonconformity is identified through internal audits, incident reports, monitoring, or any other means, it should be promptly documented and reported

3. Investigate

- The organization should conduct a thorough investigation to determine the root cause of the nonconformity. This may involve gathering evidence, conducting interviews

4. Control the Nonconformity:

- Immediate actions should be taken to control the nonconformity. This may include isolating affected systems

5. Corrective Actions:

- Develop and implement a corrective action plan to eliminate the root cause of the nonconformity. Corrective actions aim to prevent the issue from recurring
- conducting follow-up audits or assessments to confirm that the corrective actions were successful.

6. Documentation:

- Document all actions taken to correct the nonconformity, including the root cause analysis, corrective actions, and verification of their effectiveness.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

- After taking corrective actions and making enhancements, the organization returns to the planning phase to identify new areas for improvement and set new objectives
- Senior management should regularly assess the effectiveness of the ISMS
- Verify that information security policies and procedures are regularly reviewed and updated in response to changing threats
- Review of risk assessments and risk treatment plans
- Investigate whether the organization has established mechanisms for feedback from employees, customers, and other stakeholders regarding information security

Auditing (Annex A)

Item	Details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-011
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	5.1.1 Policies for information security
How to verify	° Review of ISP documents ° Interviews with a sample of users
Proof	Documents de ISP approuvées par la DG
Details of Finding	the organization has not established a formal set of information security policies that cover all relevant aspects of information security. While some policies may exist, they are either outdated, incomplete, or not formally approved by management. the policies have not been adequately communicated to employees, leaving them unaware of their responsibilities and the organization's expectations regarding information security. There is also no evidence of policies being shared with relevant external parties such as vendors, clients, or business partners
Impact	The absence of well-defined and communicated information security policies poses a significant risk to the organization's information assets and increases the likelihood of security incidents. Employees may not be aware of their roles and responsibilities in safeguarding sensitive information, leading to potential violations, data breaches, or non-compliance with legal and regulatory requirements. Additionally, the lack of policies shared with external parties may result in misalignment of security expectations and potential vulnerabilities arising from inadequate security practices by those parties
Recommandation	It is recommended that the organization promptly establish a comprehensive set of information security policies that address the organization's specific needs and risks. These policies should be approved by management, regularly reviewed, and updated as necessary. Additionally, a formal process should be implemented to ensure effective communication and awareness of the policies among employees and relevant external parties. This can include distributing the policies through appropriate channels, conducting training sessions, and obtaining acknowledgment of policy understanding and compliance from employees.

Item	Details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-012
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	6.1.1 Information security roles and responsibilities
How to verify	Review of the organizational chart
Proof	Officiel designation of differents IT responsabilties
Details of Finding	The organization does not have clearly defined information security responsibilities for its employees and stakeholders. There is no documented assignment of roles and responsibilities regarding information security-related tasks, such as risk management, incident response, access control, and security awareness training
Impact	inconsistent implementation of security measures and potential gaps in the organization's overall security posture It becomes difficult to determine who is responsible for implementing and maintaining specific security controls Different individuals or departments may interpret their responsibilities differently, resulting in variations in security practices and leaving potential vulnerabilities unaddressed. critical tasks being overlooked or neglected. This increases the organization's exposure to various risks, including data breaches, unauthorized access, system vulnerabilities, and non-compliance with regulatory requirements
Recommandation	Clearly define the responsibilities of employees, managers, IT staff, and other relevant stakeholders. Document these responsibilities in a formal policy or procedure document that is easily accessible to all employees Effective communication is crucial to ensure that all employees are aware of their information security responsibilities. Conduct regular training and awareness programs to educate employees about their roles

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-014
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	6.1.3 Contact with authorities
How to verify	Review the list of authorities
Proof	Exchange procedure with authorities
Details of Finding	The organization does not have procedures in place to specify when and by whom authorities should be contacted, and there is no clear process for reporting identified information security incidents in a timely manner
Impact	delayed or ineffective response to incidents
Recommandation	Create a comprehensive set of procedures that outline the steps to be followed when information security incidents occur. These procedures should include clear guidelines on when and how to involve authorities, such as law enforcement, regulatory bodies, or supervisory authorities Establish clear reporting channels and mechanisms for employees and stakeholders to report information security incidents. This can include designated contact points, incident reporting forms

Item	Details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-015
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	6.1.5 Information security in project management
How to verify	Review of the risk analysis document
Proof	the risk analysis document
Details of Finding	Project managers and teams do not adequately consider or address information security risks during project planning, execution, and evaluation phases
Impact	failure to address security concerns in project deliverables, leading to potential breaches, data loss, or unauthorized access
Recommandation	Develop and communicate a clear policy or guideline that emphasizes the integration of information security into project management processes. This should highlight the importance of identifying and addressing information security risks at each stage of the project lifecycle Provide training and awareness sessions to project managers and project teams, emphasizing their responsibility to consider and address information security requirements and risks Establish a formal process or checklist for project managers to follow include requirements such as conducting a thorough risk assessment, defining security objectives and deliverables, implementing appropriate security controls, and conducting periodic security reviews throughout the project lifecycle

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-016
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	6.2 Mobile devices and teleworking
How to verify	Review of the usage policy mobile devices Review of ACL
Proof	Inventory of detection and control tools for these devices
Details of Finding	The organization does not have a documented policy or adequate security measures in place to manage the risks associated with using mobile devices. Employees are allowed to connect their personal devices to the organization's network without proper security controls
Impact	Without a policy and supporting security measures, the organization is exposed to various risks associated with mobile devices. These risks include unauthorized access to sensitive information, data breaches due to lost or stolen devices, and malware infections spreading from mobile devices to the organizational network. The lack of controls increases the likelihood of security incidents and compromises the confidentiality, integrity, and availability of sensitive data
Recommandation	Create a policy that clearly outlines acceptable use, security requirements, and responsibilities for employees using mobile devices. The policy should cover aspects such as device registration, password requirements, encryption, device loss or theft reporting procedures, and restrictions on unauthorized app installations Deploy mobile device management (MDM) or enterprise mobility management (EMM) solutions to enforce security policies and controls on mobile devices Conduct regular security awareness training sessions to educate employees on the risks associated with mobile device usage

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-018
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	7.1.1 Screening
How to verify	Review of the recruitment file of one of the
Proof	recruitment procedure
Details of Finding	The organization does not conduct background verification checks on candidates for employment
Impact	Without proper background verification checks, the organization exposes itself to various risks, such as hiring individuals with a history of fraudulent activities, criminal records, or inadequate qualifications. This can lead to potential insider threats, data breaches, reputational damage, and non-compliance with legal and regulatory requirements
Recommandation	Create a policy that outlines the organization's requirements for conducting background verification checks. The policy should specify the relevant laws, regulations, and ethics that need to be followed, as well as the factors to consider in determining the level of checks based on business requirements, information classification, and perceived risks Clearly define the scope of background verification checks, including the types of checks to be performed (e.g., criminal records, employment history, educational qualifications) and the specific criteria for each check. Ensure that the criteria are directly related to the job requirements and the sensitivity of the information to be accessed

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-019
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	7.1.2 Terms and conditions of employment
How to verify	Review of Non-Disclosure Agreement
Proof	Non-Disclosure Agreement
Details of Finding	The organization's contractual agreements with employees and contractors do not explicitly state their respective responsibilities for information security. The contracts primarily focus on other aspects of the working relationship, such as compensation and job duties, without addressing information security obligations
Impact	The absence of clear information security responsibilities in contractual agreements can lead to misunderstandings and misalignment between the organization and its employees or contractors. It may result in a lack of accountability for information security, increased risk of data breaches or insider threats, and difficulties in enforcing security policies and practices
Recommandation	The organization should review and update its contractual agreements with employees and contractors to include explicit provisions regarding information security responsibilities. This can be achieved by collaborating with legal and HR departments to incorporate clauses that outline expectations for safeguarding sensitive information

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-020
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	7.2.1 Management responsibilities
How to verify	Review of the internal note signed by the CEO
Proof	the internal note signed by the CEO
Details of Finding	The organization does not have a mechanism in place to ensure that all employees and contractors consistently apply information security in accordance with the established policies and procedures. There is no clear enforcement or monitoring of adherence to these security requirements
Impact	The lack of consistent application of information security policies and procedures increases the organization's vulnerability to security incidents. It may lead to unauthorized access, data breaches, and other security incidents that could result in financial losses, reputational damage, and legal or regulatory consequences
Recommandation	Implement a comprehensive awareness program to educate employees and contractors about the importance of information security and the specific policies and procedures in place. This should include regular training sessions, workshops

Type of Finding	Non-conformity (NC)/major
Finding ID	NC-020
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	7.2.2 Information security awareness, education and training
How to verify	Review of training programs and awareness sessions
Proof	training programs and awareness sessions
Details of Finding	The organization does not have a formal awareness education and training program in place for employees and contractors, resulting in a lack of awareness among staff about their roles and responsibilities in relation to information security
Impact	The lack of appropriate awareness education and training increases the risk of employees and contractors being unaware of security policies, procedures, and best practices. This may lead to accidental or intentional security breaches, ineffective incident response, and a general lack of security-conscious culture within the organization. It can also result in non-compliance with legal, regulatory, and contractual requirements
Recommandation	The organization should establish a comprehensive awareness education and training program that covers information security policies, procedures, and best practices. The program should be tailored to different job functions and roles within the organization. Regular updates and refresher sessions should be provided to ensure that employees and contractors stay up to date with evolving security requirements. The program should include a mix of training formats, such as e-learning modules, workshops, and awareness campaigns, to effectively engage and educate the workforce. Additionally, the organization should maintain records of training completion and periodically evaluate the effectiveness of the program through assessments or surveys

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-022
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	7.2.3 Disciplinary process
How to verify	Review of the statute and rules
Proof	the statute and rules
Details of Finding	The organization does not have a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach
Impact	The lack of a formal disciplinary process can lead to inconsistent or ineffective actions being taken against employees who violate information security policies. This can result in a failure to address the root causes of security breaches and may not deter future incidents. It can also create a perception of leniency or lack of seriousness regarding information security, potentially diminishing the overall security culture within the organization
Recommandation	Establish a clear and documented procedure that outlines the steps to be followed when addressing information security breaches by employees. This process should define the roles and responsibilities of relevant stakeholders, such as HR, IT, and management, and outline the actions to be taken at each stage of the disciplinary process Ensure that the disciplinary process is effectively communicated to all employees through various channels such as employee handbooks, information security training programs, and awareness campaigns. This will help to raise awareness about the consequences of information security breaches and create a culture of accountability

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-023
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	7.3.1 Termination or change of employment responsibilities
How to verify	Verification of the deletion or adjustment of rights
Proof	Statement of assets and access rights returned following the end or modification of an employee's contract
Details of Finding	The organization does not have a process in place to define, communicate, and enforce information security responsibilities and duties that remain valid after termination or change of employment
Impact	Without clearly defined and communicated responsibilities, former employees or contractors may still have access to sensitive information or systems, increasing the risk of unauthorized access and potential data breaches
Recommandation	Create a documented policy that clearly defines information security responsibilities and duties that remain valid after termination or change of employment. The policy should include provisions for access revocation, return of assets, and any ongoing security obligations Enforce access controls that revoke or modify system privileges promptly upon termination or change of employment. Regularly review and update user access rights to align with the current roles and responsibilities Establish clear exit procedures that include the return of physical and electronic assets, removal of system access, and reminders of ongoing security obligations. Ensure that these procedures are followed consistently for all employees and contractors upon termination or change of employment

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-024
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.1.1 Inventory of assets
How to verify	Review of the inventory and verification of its completeness
Proof	Asset inventory
Details of Finding	the organization does not have a comprehensive inventory of assets associated with information and information processing facilities. There is a lack of formal documentation or system to track and maintain an up-to-date inventory of assets
Impact	The absence of an asset inventory poses several risks to the organization's information security posture. Without an accurate record of assets, it becomes challenging to manage and protect them effectively. It can lead to asset mismanagement, increased vulnerability to attacks, difficulties in incident response, and inadequate allocation of resources for asset protection
Recommandation	Develop and implement a formal asset management process that includes the identification, classification, and tracking of all assets associated with information Identify and document all hardware, software, network components, databases, and other relevant assets. Include details such as asset descriptions, unique identifiers, owners, locations, and associated risks Establish a centralized repository or system to store and maintain the asset inventory. This could be a dedicated asset management tool Assign ownership and accountability for each asset category or type. Clearly define the roles and responsibilities of individuals or teams responsible for maintaining and protecting the assets. This includes ensuring proper access controls, regular reviews, and appropriate disposal procedures when assets reach their end-of-life

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-024
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.1.2 Ownership of assets
How to verify	Review of the inventory and verification of the existence of the name of the owner
Proof	Asset inventory
Details of Finding	During the audit, it was identified that several assets in the organization's inventory are not clearly assigned ownership. The ownership information for these assets is either missing or outdated, making it difficult to determine the responsible individual or department
Impact	The lack of ownership for assets in the inventory can lead to various security and operational risks. Without clear ownership, there is a higher probability of assets being misused, mishandled, or overlooked for necessary maintenance and updates. It also hampers accountability and complicates incident response efforts, as there may be ambiguity regarding who is responsible for addressing issues related to specific assets
Recommandation	Review the organization's asset inventory and ensure that each asset is assigned a clear owner. This information should include the individual or department responsible for the asset's security, maintenance, and ongoing monitoring Establish a formal process that outlines the steps for assigning ownership to newly acquired assets Conduct periodic reviews of the asset inventory to ensure that ownership information remains accurate and up to date. Implement a mechanism to capture changes in ownership promptly, such as when an employee changes roles or leaves the organization

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-025
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.1.3 Acceptable use of assets
How to verify	Review of the correct use of information policy
Proof	the correct use of information policy
Details of Finding	There are no clear guidelines or policies in place to govern how employees should handle and protect sensitive information and assets
Impact	Without clear guidelines, employees may unknowingly engage in risky behaviors or misuse information and assets, leading to security breaches and unauthorized access Absence of rules can result in improper handling of sensitive information, increasing the likelihood of data leakage, loss, or unauthorized disclosure Security incidents resulting from improper use of information and assets can damage the organization's reputation
Recommandation	Create a comprehensive policy that outlines the rules and guidelines for acceptable use of information and assets. This policy should cover areas such as data handling, access controls, password usage Ensure the policy is properly documented, clearly stating the expectations and responsibilities of employees regarding the use and protection of information and assets. It should be easily accessible to all employees

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-026
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.1.4 Return of assets
How to verify	Review Handover Report
Proof	Handover Report
Details of Finding	several terminated employees and external party users still had organizational assets in their possession, such as company laptops, access cards, and confidential documents. There is no documented process in place to ensure the return of these assets upon termination
Impact	The lack of asset return upon termination poses significant risks to information security and confidentiality. It increases the likelihood of unauthorized access to sensitive information, potential data breaches, and misuse of company resources. It also makes it difficult to track and manage the organization's assets, leading to potential financial losses and reputational damage
Recommandation	Develop a comprehensive policy that explicitly states the requirement for all employees and external party users to return organizational assets upon termination. This policy should outline the specific procedures and timelines for asset return Ensure that all termination checklists include a step to collect and verify the return of all company assets Introduce a system or process to track and monitor the issuance and return of organizational assets. This could include asset tags, asset registers, or digital systems to maintain a record of all assets assigned to employees and external parties

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-026
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.2.1 Classification of information
How to verify	Review of asset classification procedures
Proof	Asset classification procedures
Details of Finding	The organization does not have a formal classification process for information assets. There is no systematic approach to categorizing information based on legal requirements, value, criticality, or sensitivity to unauthorized disclosure or modification
Impact	Without a proper classification process, the organization faces several risks. The lack of clarity regarding the sensitivity and criticality of information assets can lead to inadequate protection measures
Recommandation	It is recommended that the organization establishes a comprehensive information classification framework. This framework should include clear guidelines and criteria for classifying information assets based on legal requirements, value, criticality, and sensitivity. The organization should define different classification levels or categories and ensure that employees are trained on the proper handling, storage, and protection measures associated with each classification level. Additionally, regular audits and reviews should be conducted to ensure that information assets are appropriately classified and that security controls are aligned with the identified classifications

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-027
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.2.2 Labelling of information
How to verify	Verification of marking on a sample of documents
Proof	sample of documents
Details of Finding	The organization does not have appropriate procedures for information labeling in accordance with the adopted information classification scheme
Impact	The lack of proper information labeling procedures can lead to confusion and mishandling of sensitive information. Without clear labels indicating the classification level of information, there is an increased risk of unauthorized access, improper storage, and potential data breaches. It becomes difficult for employees to identify the sensitivity and handling requirements of different types of information, resulting in a higher likelihood of security incidents and non-compliance with regulatory requirements
Recommandation	Create a comprehensive set of procedures that outline how information should be labeled based on the organization's information The procedures should clearly define the labeling requirements for each classification level, including specific labeling elements (e.g., headers, footers, watermarks) and placement on physical and electronic documents Conduct training sessions to educate employees on the importance of information labeling, the meaning of different classification levels Ensure that the labels used accurately reflect the classification levels assigned to different types of information

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-028
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.3.1 Management of removable media
How to verify	Testing the use of removable media drives on a sample of workstations
Proof	Procedures for managing removable media
Details of Finding	There are no specific guidelines or controls governing the use, storage, and disposal of removable media based on their classification
Impact	The lack of appropriate procedures for managing removable media according to the classification scheme poses several risks. It increases the potential for unauthorized access to sensitive information if media falls into the wrong hands
Recommandation	Create a policy that outlines the proper handling, usage, storage, and disposal of removable media based on the organization's classification scheme. This policy should include guidelines for encryption, access controls, and labeling of media Conduct awareness and training programs to ensure that employees understand the importance of managing removable media according to the classification scheme. Train them on the proper procedures for handling different types of media based on their sensitivity level Implement authentication mechanisms such as passwords or smart cards to ensure that only authorized personnel can use and access the media Implement measures such as locked cabinets or secure containers to prevent unauthorized access. Establish guidelines for transporting media between locations to minimize the risk of loss or theft Establish procedures for the secure disposal of removable media at the end of its lifecycle. This may involve secure wiping, degaussing, or physical destruction methods

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-029
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.3.2 Disposal of media
How to verify	Review disposal document
Proof	Disposal document
Details of Finding	The organization does not have formal procedures in place for the secure disposal of media when it is no longer required. There are no documented guidelines or processes outlining the proper disposal methods
Impact	The lack of formal procedures for media disposal increases the risk of unauthorized access to sensitive information. Media containing confidential data, such as hard drives, tapes, or USB drives, may be discarded without proper erasure or destruction, making the organization susceptible to data breaches and potential regulatory non-compliance
Recommandation	establish and implement formal procedures for the secure disposal of media. These procedures should include guidelines for the proper erasure, destruction, or recycling of different types of media. The recommended actions may include using secure wiping software for digital media, physically destroying physical media using approved methods (e.g., shredding or degaussing), and ensuring that all disposal activities are documented and auditable the organization should provide training and awareness programs to employees to ensure they are aware of the media disposal procedures and understand the importance of securely disposing of media when it is no longer required. Regular monitoring and compliance checks should be conducted to verify adherence to the established procedures

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-030
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	8.3.3 Physical media transfer
How to verify	Review of transport records
Proof	transport records
Details of Finding	the organization does not have any specific measures in place to protect media containing sensitive information during transportation. There are no documented procedures or controls addressing the secure transportation of physical media, such as backup tapes or portable hard drives
Impact	The lack of protection for media during transportation increases the risk of unauthorized access, misuse, or corruption. If sensitive information falls into the wrong hands or gets corrupted during transportation, it could lead to a breach of confidentiality, loss of data integrity, and potential regulatory compliance violations. It may also result in reputational damage for the organization
Recommandation	Develop a documented policy and procedures specifically addressing the secure transportation of media containing sensitive information. This should include guidelines for packaging, labeling, and tracking media, as well as ensuring appropriate physical security during transportation Implement controls such as tamper-evident packaging, encryption, or secure courier services to protect media from unauthorized access, misuse, or corruption during transportation

Type of Finding	Non-conformity (NC)/major
Finding ID	NC-031
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.1.1 Access control policy
How to verify	Access control policy review
Proof	Access control policy
Details of Finding	The organization does not have an established and documented access control policy that is regularly reviewed based on business and information security requirements
Impact	The lack of a policy can result in inconsistent application of access controls across systems and assets. This can lead to unauthorized access, data breaches, and potential compromise of sensitive information, may result in penalties, legal consequences, and damage to the organization's reputation This increases the likelihood of security incidents, such as unauthorized access, data leaks, or insider threats.
Recommandation	Develop a comprehensive access control policy that clearly defines the principles, objectives, and requirements for granting and managing user access to systems and information assets Set up a process to periodically review the access control policy to ensure its alignment with changing business needs and evolving security risks regular audits, access reviews Conduct training sessions and awareness programs to ensure employees understand the access control policy, their responsibilities, and the importance of compliance

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-032
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.1.2 Access to networks and network services
How to verify	Review ACL Firewall rules
Proof	ACL, Firewall Rules
Details of Finding	During the audit, it was identified that certain users have been granted unauthorized access to the network and network services beyond what they have been explicitly authorized to use. This includes access to sensitive systems and data that is not within their job responsibilities
Impact	Unauthorized access exposes sensitive information to potential misuse, increases the likelihood of data breaches, and compromises the confidentiality, integrity, and availability of critical systems and data. It also creates a potential insider threat and increases the risk of unauthorized changes or malicious activities
Recommandation	Conduct a thorough access review to identify and revoke any unauthorized access privileges granted to users. This should include a comparison of user access rights against their job responsibilities and the principle of least privilege Implement RBAC to ensure that user access is based on defined roles and responsibilities. This will help enforce the principle of least privilege and prevent users from having unnecessary access to network resources Develop and enforce comprehensive access control policies and procedures that clearly define the authorization process for granting access rights. This should include a formal request, approval, and provisioning process, as well as periodic reviews and audits to ensure compliance

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-033
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.1 User registration and de-registration
How to verify	Verification of user accounts on servers to identify those that are redundant or obsolete
Proof	List of user accounts on servers
Details of Finding	There is no systematic method to assign access rights to users or identify and remove/disable redundant user IDs
Impact	This increases the risk of unauthorized individuals gaining access to sensitive information or critical systems Failure to periodically identify and remove/disable redundant user IDs leads to a proliferation of unnecessary accounts in the system. This not only consumes resources but also increases the attack surface and the potential for misuse of these accounts In case of security incidents or policy violations, it becomes challenging to attribute actions to specific individuals, hindering investigations and accountability
Recommandation	Implement a documented user registration and de-registration process that outlines the steps, responsibilities, and required approvals for granting and revoking user access rights Conduct periodic reviews to identify redundant user accounts and disable or remove them from the system. This can be done through a combination of automated tools and manual verification Utilize access control mechanisms, such as role-based access control (RBAC), to ensure that users are granted the appropriate access rights based on their roles and responsibilities Implement auditing mechanisms to monitor and track user access activities

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-034
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.2 User access provisioning
How to verify	Review of access rights matrices and job descriptions
Proof	Review of access rights matrices and job descriptions
Details of Finding	Access rights for users are assigned and revoked inconsistently, and there is no standardized procedure for granting or revoking access across systems and services
Impact	Users may have inappropriate access privileges, leading to potential data breaches or unauthorized activities Without a standardized process, managing access rights becomes time-consuming and error-prone, increasing the burden on administrators The organization may struggle to demonstrate proper control over user access, which can result in compliance failures and audit findings
Recommandation	Develop a documented process that outlines the steps for requesting, approving, and provisioning access rights to systems and services. This process should cover all user types, including employees, contractors, and third-party users Implement RBAC to assign access rights based on predefined roles and responsibilities. This approach ensures that users are granted the appropriate level of access based on their job functions Conduct periodic access reviews to ensure that access rights are still relevant and necessary for each user. Remove or modify access rights as required based on job changes, terminations, or changes in responsibilities

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-035
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.3 Management of privileged access rights
How to verify	Review log access
Proof	Log access
Details of Finding	There are instances where individuals have unauthorized or excessive privileges, granting them unrestricted access to sensitive systems and data
Impact	The lack of control over privileged access rights increases the risk of unauthorized activities, data breaches, and malicious insider threats. It can lead to unauthorized modification or disclosure of critical information, compromising the confidentiality, integrity, and availability of systems and data. The organization's reputation, customer trust, and compliance with regulatory requirements may also be at stake
Recommandation	Implement a RBAC model that defines roles and associated privileges based on job responsibilities Enforce the principle of least privilege by separating administrative and user privileges Establish a formal process for requesting and approving privileged access rights. Implement a documented workflow for access requests, including appropriate authorization and justification. Ensure that access requests are reviewed and approved by the relevant stakeholders, such as managers or data owners Implement robust monitoring and auditing mechanisms to track and log privileged access activities. Monitor and analyze access logs regularly to detect any unauthorized or suspicious activities. Establish alert mechanisms to notify relevant personnel in real-time when anomalies are detected centralize the management of privileged accounts

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.5 Review of user access rights
How to verify	Review of the access rights matrix of a sample of users who have changed status
Proof	Account change logs
Details of Finding	The organization fails to conduct regular reviews of users' access rights as required by the control
Impact	Users may retain access rights to sensitive systems or data that they no longer require, increasing the risk of unauthorized access, data breaches, or misuse
Recommandation	Implement a formal process to regularly review and revoke unnecessary access rights for users. This could involve conducting access reviews quarterly or annually

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.6 Removal or adjustment of access rights
How to verify	Verification on the servers of the deletion or adjustment of access rights of those who have left or whose contracts have changed
Proof	History of changes to access rights
Details of Finding	Failure to adjust access rights for external party users when their contract or agreement ends. Access rights remain unchanged when an employee's role or responsibilities change within the organization
Impact	External parties who no longer have a legitimate need for access can continue to access sensitive information or systems, increasing the risk of data breaches, unauthorized activities, or misuse of resource
Recommandation	Develop a comprehensive procedure to regularly review and adjust access rights for external party users. This process should involve periodic audits, contract-based access control mechanisms, and timely communication between relevant stakeholders (e.g., HR, procurement, and IT departments)

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.4.1 Information access restriction
How to verify	Verification of ACLs on network and security equipment
Proof	Logs des accès
Details of Finding	Employees have unrestricted access to sensitive data and application functions without any restrictions or authorization procedures in place
Impact	Without proper access controls, individuals could gain unauthorized access to sensitive information and application functions, leading to data breaches, data loss, or misuse of resources Lack of restrictions can result in unauthorized modifications, deletions, or disclosure of sensitive information, compromising its integrity and confidentiality Non-compliance with access control policies may result in legal repercussions, regulatory fines, or damage to the organization's reputation
Recommandation	Develop a comprehensive access control policy that defines roles, responsibilities, and procedures for granting and revoking access to information and application system functions Implement strong authentication mechanisms such as passwords, two-factor authentication, or biometrics to verify users' identities. Use authorization mechanisms to grant access based on authenticated user roles and privileges

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-036
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.4 Management of secret authentication information of users
How to verify	Access testing on systems and software using secret default authentication credentials
Proof	Screenshots of login attempts using default authentication credentials
Details of Finding	organization does not have a formal management process in place for allocating secret authentication information. Instead, individual employees are responsible for creating and managing their own passwords without any oversight or control
Impact	Without a formal management process, there is a higher likelihood of weak or easily guessable passwords, password reuse, or unauthorized access to systems and data
Recommandation	Establish a documented process for the allocation of secret authentication information. This process should define the criteria for generating strong passwords, specify who is responsible for generating and managing them, and outline procedures for secure distribution and storage Develop and enforce password policies that specify complexity requirements, expiration periods, and restrictions on password reuse. This helps ensure that secret authentication information remains confidential and secure Implement a role-based access control (RBAC) system that assigns appropriate access privileges based on job roles and responsibilities. This helps prevent unauthorized access and ensures that individuals have access only to the resources they need

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.2.6 Removal or adjustment of access rights
How to verify	Verification on the servers of the deletion or adjustment of access rights of those who have left or whose contracts have changed
Proof	History of changes to access rights
Details of Finding	Failure to adjust access rights for external party users when their contract or agreement ends. Access rights remain unchanged when an employee's role or responsibilities change within the organization
Impact	External parties who no longer have a legitimate need for access can continue to access sensitive information or systems, increasing the risk of data breaches, unauthorized activities, or misuse of resource
Recommandation	Develop a comprehensive procedure to regularly review and adjust access rights for external party users. This process should involve periodic audits, contract-based access control mechanisms, and timely communication between relevant stakeholders (e.g., HR, procurement, and IT departments)

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.4.2 Secure log-on procedures
How to verify	Verification on the systems: connection blocking after a certain number of failed attempts , Successful and failed access attempts logged
Proof	log des accès
Details of Finding	there is no requirement for employees to use secure log-on procedures when accessing systems and applications. Instead, individuals can freely access these resources without any authentication or password protection
Impact	Without a secure log-on procedure, anyone can potentially gain unauthorized access to sensitive systems and applications, leading to data breaches, information leaks, or malicious activities Without individual user identification and authentication, it becomes difficult to track and attribute actions performed within the systems, hindering forensic investigations and accountability
Recommandation	Develop and enforce a comprehensive access control policy that clearly defines the requirements for secure log-on procedures Implement robust authentication mechanisms such as two-factor authentication (2FA) or multi-factor authentication (MFA). This ensures that individuals must provide multiple forms of identification (e.g., passwords, tokens, biometrics) before accessing systems and application

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.4.3 Password management system
How to verify	Verify password configuration settings on servers, databases, applications and network and security equipment
Proof	screenshot
Details of Finding	the password management system in place does not enforce quality passwords and lacks interactivity. Employees are allowed to set weak passwords with easily guessable phrases, such as "password123" or their own name. Additionally, the system does not prompt users to change passwords periodically or provide guidance on creating strong passwords
Impact	Weak passwords are easier to guess or crack, providing an opportunity for malicious individuals to gain unauthorized access to sensitive information or systems
Recommandation	Implement a password policy that mandates the use of strong passwords with a combination of alphanumeric characters, symbols, and a minimum length. This ensures that passwords are harder to guess or crack Configure the password management system to prompt users to change their passwords periodically, such as every 90 days. This reduces the risk of long-term exposure to a compromised password Offer guidelines and training to educate employees on creating strong passwords and the importance of password security

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.4.4 Use of privileged utility programs
How to verify	check usage logs of privileged utility programs
Proof	logs of privileged utility programs
Details of Finding	employees are granted unrestricted access to utility programs that can override system and application controls. These utility programs are not tightly controlled or restricted, allowing users to manipulate and bypass security measures
Impact	Unrestricted access to utility programs increases the likelihood of unauthorized system modifications, data breaches, or malicious activities. It may lead to unauthorized changes to critical configurations, unauthorized access to sensitive information, or the introduction of malware or malicious code
Recommandation	Implement strict access controls and restrictions on utility programs. Only authorized personnel should have access to these programs based on their roles and responsibilities Establish a formal authorization process that requires appropriate approvals and documentation for granting access to utility programs. This ensures that access is granted only to individuals who have a legitimate need and are accountable for their actions Implement robust logging and monitoring mechanisms to track and record activities related to utility programs

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	9.4.5 Access control to program source code
How to verify	verification of access logs
Proof	access logs
Details of Finding	the source code repository is accessible to all employees without any restrictions. Any employee can view, modify, or copy the source code of the organization's software applications without proper authorization
Impact	Unrestricted access to program source code increases the risk of intellectual property theft. Competitors or malicious insiders can easily access and steal valuable source code, compromising the organization's competitive advantage
Recommandation	Implement access control mechanisms, such as role-based access control (RBAC) or access control lists (ACLs), to restrict access to the program source code. Only authorized individuals or teams should have the necessary privileges to view, modify, or copy the source code

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	10.1.1 Policy on the use of cryptographic controls
How to verify	Review of the policy for the use of cryptographic measures
Proof	policy for the use of cryptographic measures
Details of Finding	organization has not developed and implemented a policy on the use of cryptographic controls for protecting information. There are no guidelines or procedures in place regarding the use of encryption techniques to secure sensitive data
Impact	Without a policy in place, there is a higher risk of unauthorized access, data breaches, and compromised confidentiality. Sensitive information could be exposed to malicious actors, leading to reputational damage, financial losses, legal consequences, and loss of customer trust
Recommandation	Create a comprehensive policy that outlines the organization's requirements and guidelines for the use of cryptographic controls. This policy should address the types of encryption algorithms to be used, key management procedures, encryption protocols Once the policy is defined, implement appropriate encryption mechanisms across the organization's systems and networks. This could involve deploying encryption software, hardware-based encryption modules, or utilizing encryption features provided by various technologies and applications

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	10.1.2 Key management
How to verify	Review of the policy on the use, protection and lifetime of cryptographic keys
Proof	policy on the use, protection and lifetime of cryptographic keys
Details of Finding	there is no policy in place regarding the use, protection, and lifetime of cryptographic keys. Employees are unaware of the importance of managing cryptographic keys securely and the organization does not have any specific guidelines or procedures for key generation, distribution, storage, rotation, and destruction
Impact	Without a proper policy, cryptographic keys may be weak or vulnerable, leading to potential unauthorized access or data breaches
Recommandation	Create a policy that covers the entire lifecycle of cryptographic keys, including key generation, distribution, storage, rotation, and destruction Establish clear procedures for key generation, distribution, storage, rotation, and destruction. These procedures should address how keys are securely generated, securely distributed to authorized users, stored in a protected manner, regularly rotated, and properly destroyed when no longer needed

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.1 Secure areas
How to verify	Visual inspection of security perimeters
Proof	pictures
Details of Finding	there are no clearly defined security perimeters in place to protect areas that contain sensitive or critical information and information processing facilities. Employees have unrestricted access to these areas, and there are no physical or logical controls in place to prevent unauthorized access
Impact	increases the risk of unauthorized access to sensitive or critical information, leading to potential data breaches. It also increases the risk of physical damage or theft of information processing facilities, such as servers or data storage devices
Recommandation	Clearly define the boundaries of areas that contain sensitive or critical information and information processing facilities. This can include physical areas (e.g., data centers, server rooms)

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.1.2 Physical entry controls
How to verify	Visitor record check
Proof	Record check
Details of Finding	there is a server room that stores sensitive data, but it does not have any entry controls. Anyone can freely enter the server room without authorization or identification
Impact	Unauthorized individuals, including employees, contractors, or even external threats, can gain access to the server room. This increases the likelihood of unauthorized data access, tampering, theft, or sabotage, potentially leading to data breaches, financial loss, reputational damage, or regulatory compliance issues
Recommandation	Install appropriate entry controls such as access cards, biometric systems, or locks with restricted key distribution. These measures ensure that only authorized personnel with the necessary credentials can access the secure areas

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.1.3 Securing offices, rooms and facilities
How to verify	Visual inspection
Proof	architectural plan of the auditee's building
Details of Finding	the physical security control for offices, rooms, and facilities is not properly implemented. Doors to sensitive areas are left unlocked, visitors are not properly monitored, and there are no surveillance cameras or access control systems in place
Impact	The lack of physical security measures can lead to unauthorized access to sensitive areas, theft of valuable equipment or information, and potential disruptions to business operations. It increases the risk of physical breaches, compromises confidentiality, and potentially damages the company's reputation
Recommandation	Implement access control systems such as card readers, biometric scanners, or PIN codes to restrict entry to authorized personnel only Install surveillance cameras in strategic locations to monitor and record activities within the offices, rooms, and facilities Implement a visitor management system that requires visitors to sign in, wear visible identification badges, and be accompanied by authorized personnel while on the premises Ensure that doors to sensitive areas are equipped with appropriate locking mechanisms, such as electronic locks or keycard access

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.1.4 Protecting against external and environmental threats
How to verify	Verification of the location of humidity and leak detectors water and smoke
Proof	Detection systems test reports and fire extinguisher
Details of Finding	Failure to implement appropriate physical protection measures to mitigate the risk of natural disasters or malicious attacks. For instance, a company's data center is located in a flood-prone area, but no preventive measures such as flood barriers or elevated server racks are in place
Impact	In the event of a flood, the data center could experience severe damage or complete destruction. This would result in the loss of critical systems, data, and potential service disruptions for the organization. It may also lead to reputational damage and financial losses due to downtime
Recommandation	Conduct a comprehensive risk assessment to identify potential threats, vulnerabilities, and their potential impact on the physical security of the data center Implement appropriate physical security controls based on the identified risks. This may include flood barriers, water detection systems, raised flooring, or relocating the data center to a safer location Install fire suppression systems, smoke detectors, and fire-resistant materials to minimize the risk of fire-related damage. Regularly test and maintain these systems to ensure their effectiveness Deploy robust intrusion detection systems, video surveillance, access controls, and alarm systems to detect and deter malicious attacks or unauthorized access to the data center Develop a comprehensive business continuity and disaster recovery plan that includes provisions for physical security incidents. This plan should outline response procedures, backup strategies, alternative site arrangements, and communication protocols

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.1.5 Working in secure areas
How to verify	Review of procedures for working in secure areas
Proof	procedures for working in secure areas
Details of Finding	there is no clear procedure in place for employees to follow when working in secure areas. Employees are not provided with guidelines or instructions on how to handle sensitive information within these areas
Impact	Without proper procedures, employees may unknowingly mishandle sensitive data or leave it exposed, increasing the likelihood of unauthorized access or data breaches Without established procedures, employees may adopt their own methods for working in secure areas, leading to inconsistent security practices across the organization.
Recommandation	Create a set of clear and documented procedures for working in secure areas. These procedures should cover aspects such as access control, handling of sensitive information, use of electronic devices, and visitor management Establish a system to monitor and supervise activities within secure areas. This can include CCTV cameras, security personnel, or periodic audits to ensure compliance with the procedures Define a process for reporting and responding to security incidents or violations within secure areas

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.1.6 Delivery and loading areas
How to verify	Visit and inspection of the loading and delivery area
Proof	pictures
Details of Finding	the access points such as delivery and loading areas are not adequately controlled or isolated from information processing facilities. Unauthorized individuals can freely enter the premises and gain unauthorized access to sensitive information
Impact	unauthorized individuals gaining physical access to critical areas where information processing takes place unauthorized access, theft, tampering, or destruction of sensitive data. It may also compromise the confidentiality, integrity, and availability of information, leading to potential financial losses, reputation damage, and regulatory non-compliance
Recommandation	Implement stringent access control measures for all access points, including delivery and loading areas. This may include the use of access control systems, such as badges, biometric authentication, or security personnel to monitor and restrict entry to authorized individuals only

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.1 Equipment siting and protection
How to verify	Verification of the means of protection of the material
Proof	Guidelines on eating, drinking and smoking near information processing facilities
Details of Finding	the server room is located in an area that is prone to flooding, and there are no measures in place to protect the equipment from potential water damage. Additionally, the server room door is not secured properly, allowing unauthorized individuals to gain access easily
Impact	In the event of a flood, the equipment could be damaged, leading to data loss and disruption of critical services. The lack of secure access also increases the chances of unauthorized individuals gaining physical access to sensitive information, potentially leading to data breaches or tampering
Recommandation	Move the server room to a secure location that is not prone to environmental threats such as flooding or extreme temperatures. This ensures the equipment is protected from potential hazards Install flood detection systems, raised flooring, and water barriers to minimize the risks associated with environmental threats

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.3 Cabling security
How to verify	Review of the wiring diagram of the electrical and computer network
Proof	wiring diagram of the electrical and computer network
Details of Finding	the power and telecommunications cabling carrying data or supporting information services are not adequately protected from interception, interference, or damage. The cabling is exposed and easily accessible to unauthorized individuals, increasing the risk of data breaches, tampering, or disruption of information services
Impact	Unauthorized individuals may gain access to sensitive data transmitted through the cabling, leading to data breaches and compromising the confidentiality of information. Interference or damage to the cabling can disrupt communication and information flow, causing downtime and affecting business operations
Recommandation	Implement physical security measures such as restricted access areas, locked cabinets, or secure enclosures to safeguard the power and telecommunications cabling. Only authorized personnel should have access to these areas Ensure that cabling is properly routed and concealed, minimizing exposure and reducing the risk of unauthorized access or damage. This can be achieved by using cable trays, conduits, or other appropriate cable management systems video surveillance, or alarms that notify security personnel of any suspicious activities

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization's practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.2 Supporting utilities
How to verify	Verification de l'existence d'alimentation redondante, d'onduleur, d'un groupe electrogene
Proof	Test reports of these services
Details of Finding	company fails to implement adequate protection measures for its equipment, such as servers, against power failures and disruptions caused by failures in supporting utilities. They may not have backup power supplies, surge protectors, or failover mechanisms in place
Impact	Power failures or disruptions can lead to equipment downtime, resulting in service disruptions, loss of productivity, and revenue loss. Power fluctuations or disruptions can damage sensitive equipment, leading to hardware failures and expensive repairs or replacements
Recommandation	Install UPS devices to provide backup power during power outages, allowing equipment to continue running or be shut down safely Implement redundant power sources, such as dual power feeds or backup generators, to ensure continuous power supply to critical equipment Install surge protectors and voltage regulators to safeguard equipment against power surges and fluctuations

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	Users should be required to follow the organization’s practices in the use of secret NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.4 Equipment maintenance
How to verify	Review of maintenance intervention reports
Proof	maintenance intervention reports
Details of Finding	the network infrastructure equipment, such as routers and switches, is not regularly maintained or updated. Firmware patches and security updates are neglected, resulting in outdated and vulnerable equipment
Impact	Outdated equipment may have known vulnerabilities that can be exploited by malicious actors, leading to unauthorized access, data breaches, or network disruptions
Recommandation	Develop a documented maintenance schedule for all equipment, including regular firmware updates, security patches

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.5 Removal of assets
How to verify	Review of asset exit registers
Proof	asset exit registers
Details of Finding	An employee at a company takes a company-owned laptop home without obtaining prior authorization. The laptop contains sensitive customer information and proprietary software. The employee uses the laptop for personal purposes, potentially exposing the data to unauthorized access, loss, or theft
Impact	If the laptop is lost, stolen, or accessed by unauthorized individuals, sensitive customer information may be compromised, leading to potential data breaches and privacy violations. The employee may install unauthorized software on the laptop, which can introduce malware or increase vulnerabilities, potentially compromising the company's information security Taking equipment off-site without proper authorization reduces the company's control over its assets and increases the risk of loss, damage, or misuse
Recommandation	Create a clear policy that explicitly states that equipment, information, or software should not be taken off-site without prior authorization. Ensure that employees are aware of this policy through regular communication and training programs Implement a formal authorization process that requires employees to obtain explicit permission from their supervisors or the appropriate authority before taking equipment off-site. This process should include justification for the request and specify any security measures to be taken Maintain an accurate inventory of company-owned equipment, including laptops, mobile devices, and other portable devices Require the use of encryption and security measures, such as strong passwords and multi-factor authentication, on all company-owned devices. This helps protect data in case of loss or theft.

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.7 Secure disposal or re-use of equipment
How to verify	Review of disposal procedure
Proof	disposal procedure
Details of Finding	Let's say a company is upgrading its computer systems and decides to dispose of some old computers. However, before disposing of the computers, they fail to verify if any sensitive data or licensed software has been removed or securely overwritten. As a result, the computers are sold or discarded without proper data sanitization measures, potentially leaving sensitive information accessible to unauthorized individuals
Impact	It can lead to unauthorized access to sensitive data, including personal information of customers, employees, or intellectual property of the organization. This can result in breaches of privacy, loss of trust from customers, legal liabilities, financial losses, and damage to the company's reputation
Recommandation	Develop and implement comprehensive procedures for data sanitization before disposing of or reusing equipment containing storage media Maintain an accurate inventory of all items of equipment containing storage media to track their lifecycle and ensure proper handling during disposal or re-use

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.8 Unattended user equipment
How to verify	Review of awareness session programs
Proof	awareness session programs
Details of Finding	A user leaves their computer unattended without activating a password-protected screensaver or locking the session
Impact	Unauthorized individuals may gain physical access to the unattended equipment and compromise sensitive information, leading to data breaches, unauthorized access, or misuse of resources. This can result in financial loss, reputational damage, and legal implications for the organization
Recommandation	Implement a robust user awareness program to educate employees about the importance of securing unattended equipment. Train them on the procedures to lock their screens or activate password-protected screensavers when stepping away from their workstations

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	11.2.9 Clear desk and clear screen policy
How to verify	Clean Desktop and Blank Screen Policy Review
Proof	screenshot
Details of Finding	Employees frequently leave sensitive papers and removable storage media, such as USB drives, on their desks overnight. They also leave their computer screens unlocked and visible when they are away from their workstations
Impact	Leaving sensitive papers and removable storage media unattended increases the risk of unauthorized individuals gaining access to confidential or sensitive information Unlocked computer screens expose sensitive information to potential data breaches. Unauthorized users can easily view or steal information from these unattended workstations
Recommandation	Enforce a policy that requires employees to clear their desks of all sensitive papers and removable storage media at the end of each working day. Provide secure storage facilities, such as lockable cabinets or drawers, where employees can store these items when not in use Employees should be trained to lock their computer screens or use screen savers with password protection whenever they step away from their workstations

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.1.4 Separation of development, testing and operational environments
How to verify	If the application servers (where the applications are installed) and BD are dedicated servers
Proof	Inventory of development and test servers
Details of Finding	the development, testing, and operational environments are not adequately separated. For example, developers have direct access to the operational environment
Impact	Developers or testers may have access to sensitive production data or systems, increasing the risk of unauthorized access or data breaches Testing activities or development work in the shared environment can accidentally introduce changes that affect the operational environment's stability, reliability, or security
Recommandation	Establish clear boundaries between development, testing, and operational environments. This can be achieved through network segmentation, virtualization, containerization, or dedicated infrastructure Enforce strict access controls to restrict and monitor access to different environments. Only authorized personnel should have access to the specific environments required for their tasks

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.2.1 Controls against malware
How to verify	Malware Protection Policy Review
Proof	Malware Protection Policy
Details of Finding	organization fails to implement effective detection, prevention, and recovery controls to protect against malware
Impact	Without adequate controls, the organization becomes more susceptible to malware attacks, such as viruses, ransomware, or trojans. This can lead to data breaches, system disruptions, and financial losses
Recommandation	Deploy antivirus software, intrusion detection and prevention systems, and email and web filtering solutions to detect and block malware. Regularly update and patch these systems to stay protected against emerging threats

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.3.1 Information backup
How to verify	Safeguard policy review
Proof	policy review
Details of Finding	the backup policy is not being followed consistently. Backup copies of information, software, and system images are not taken and tested regularly as required
Impact	If a critical system failure, data loss, or security breach occurs, the company may not have up-to-date backup copies available to restore the affected information, software, or system images. This can lead to prolonged downtime, loss of important data, and disruption of business operations
Recommandation	Make sure the backup policy is well-documented, easily accessible, and regularly reviewed and updated as necessary

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.4.1 Event logging
How to verify	Review of the logging policy
Proof	logging policy
Details of Finding	the event logs recording user activities, exceptions, faults, and information security events are not consistently produced, stored, or regularly reviewed
Impact	Without proper event logs, the organization lacks visibility into user activities and potential security incidents, making it challenging to detect and respond to security breaches in a timely manner.
Recommandation	Establish a centralized event logging system that captures and stores logs from all relevant sources, such as servers, network devices, and security appliances. This ensures comprehensive coverage and centralized management of event logs Establish clear policies on how long event logs should be retained based on regulatory requirements and business needs. This ensures that logs are available for analysis and investigations when necessary. Utilize security information and event management (SIEM) tools or log analysis solutions to automate the monitoring of event logs

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.4.2 Protection of log information
How to verify	Checking the protection mechanisms of the logging process
Proof	protection mechanisms of the logging process
Details of Finding	company has implemented logging facilities to record and store critical system logs. However, they do not have any security measures in place to protect these logs from tampering or unauthorized access. Anyone within the organization, including employees with malicious intent, can modify or delete the logs without leaving any trace
Impact	Since the logs are not protected, it becomes difficult to identify and investigate security incidents or suspicious activities. It hampers the ability to detect and respond to security breaches promptly. Furthermore, if the logs are tampered with or deleted, it can hinder forensic analysis and make it harder to identify the root cause of incidents
Recommandation	Implement access controls to restrict unauthorized access to logging facilities and log information. Only authorized personnel should have access to the logs, and access should be granted based on the principle of least privilege

Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.4.3 Administrator and operator logs
How to verify	Checking admin log protection mechanisms
Proof	admin log protection mechanisms
Details of Finding	the system administrator and system operator activities are not being logged, and the logs are not adequately protected and regularly reviewed
Impact	In the event of a security incident or breach, the absence of activity logs can make it difficult to identify the source, understand the scope of the incident, and take appropriate measures to mitigate the damage.
Recommandation	Deploy a robust logging mechanism that captures system administrator and system operator activities comprehensively. This should include relevant details such as user identities, actions performed, timestamps, and any exceptions or errors encountered

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.4.4 Clock synchronisation
How to verify	verification of the synchronization of the clocks of the servers and network and security equipment with a single NTP server
Proof	server and network equipment clocks
Details of Finding	the clocks of the information processing systems are not synchronized to a single reference time source. Different systems have their own time settings
Impact	In case of a security incident or breach, the lack of synchronized clocks can make it challenging to correlate events accurately. This can impede the investigation process and hinder the organization's ability to identify the root cause of the incident
Recommandation	Deploy a time synchronization mechanism, such as the Network Time Protocol (NTP), to synchronize the clocks of all relevant information processing systems. NTP allows systems to maintain accurate time by synchronizing with a reliable reference time source Designate a reliable time server within the organization or security domain as the single reference time source. This server should be synchronized with a highly accurate external time source, such as a national time

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.6.1 Management of technical vulnerabilities
How to verify	Review of the technical vulnerability management procedure
Proof	technical vulnerability management procedure
Details of Finding	there is a lack of established procedures to obtain information about technical vulnerabilities of the information systems being used. The organization fails to monitor and gather timely information regarding vulnerabilities present in their systems
Impact	Without timely information about technical vulnerabilities, the organization remains unaware of potential security weaknesses in their information systems. This increases the risk of exploitation by malicious actors, leading to unauthorized access, data breaches, system downtime, loss of critical information, and damage to the organization's reputation
Recommandation	Implement a formal process to monitor and track technical vulnerabilities in the information systems. This process should include regular vulnerability scanning, threat intelligence gathering, and continuous monitoring

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.6.2 Restrictions on software installation
How to verify	Review of the list of types of software whose installation is authorized
Proof	list of types of software whose installation is authorized
Details of Finding	there is no established or implemented rule governing the installation of software by users. As a result, employees have unrestricted access to install any software they want on their workstations without any control or oversight
Impact	Without proper rules and controls in place, users may unknowingly install malicious software or unapproved applications, leading to potential security breaches, data leaks, or system vulnerabilities
Recommandation	Establish a policy that clearly outlines the rules and procedures for software installation by users. Communicate the policy to all employees and ensure their understanding of the guidelines and consequences for non-compliance. Enforce user access controls to restrict installation rights to authorized personnel only. Implement mechanisms such as user permissions, group policies, or administrative approvals to control software installations

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	12.7.1 Information systems audit controls
How to verify	Review of the information systems audit procedure
Proof	information systems audit procedure
Details of Finding	the IT department decides to conduct an extensive audit of all operational systems without proper planning and agreement with the relevant business units
Impact	The disruptions caused by the unplanned and uncoordinated audit activities can lead to a loss of productivity and efficiency within the organization. Critical business processes may be temporarily halted or interrupted, resulting in delays, missed deadlines, and potential financial losses
Recommandation	Establish a well-defined process for planning and coordinating audit requirements and activities involving verification of operational systems. This should involve collaboration between the IT department, relevant business units, and other stakeholders

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	13.1.1 Network controls
How to verify	Review of the management procedure network equipment
Proof	management procedure network equipment
Details of Finding	company has an insecure wireless network with weak encryption protocols and no authentication mechanisms in place. This non-conformity means that the network is not being managed and controlled effectively to protect the information in the systems and applications.
Impact	unauthorized individuals can easily gain access to the company's network. They could intercept sensitive information transmitted over the network, such as customer data, financial records, or trade secrets. This could lead to data breaches, financial loss, reputational damage, and potential legal consequences for the company
Recommandation	Divide the network into segments or zones based on the sensitivity of the information and implement appropriate access controls between them. This helps contain potential breaches and limit unauthorized access Implement robust encryption protocols (e.g., WPA2 or WPA3 for Wi-Fi networks) to protect data transmitted over the network. This ensures that even if someone intercepts the traffic, they won't be able to decipher the informatio Implement strong authentication mechanisms, such as strong passwords or two-factor authentication, to restrict unauthorized access to the network. This ensures that only authorized individuals can connect to the network. Deploy network monitoring tools and intrusion detection systems to detect any suspicious activities or potential security breaches in real-time. This helps in identifying and mitigating threats promptly Keep network devices, such as routers and switches, up to date with the latest security patches and firmware updates. This helps address any known vulnerabilities and enhances the overall security posture of the network

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	13.1.2 Security of network services
How to verify	Review of the service level agreements (SLA) concluded with the service providers
Proof	service level agreements (SLA) concluded with the service providers
Details of Finding	there is a lack of identification and inclusion of security mechanisms, service levels, and management requirements in network services agreements. This means that the agreements fail to explicitly address these aspects
Impact	Without including such requirements in network services agreements, the organization is exposed to potential security risks and vulnerabilities. Service providers may not be contractually obligated to implement necessary security measures or meet defined service levels, leading to increased chances of unauthorized access, data breaches, or service disruptions
Recommandation	Assess the current agreements to determine if they adequately address security mechanisms, service levels, and management requirements. Identify any gaps or deficiencies Clearly define the necessary security mechanisms, such as encryption, authentication protocols, access controls, and incident response procedures, which should be included in network services agreements Determine the required service levels for network services, including availability, response times, and performance metrics. These should align with the organization's needs and be included in the agreements

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	13.1.3 Segregation in networks
How to verify	Review of the synoptic diagram of the network architecture
Proof	synoptic diagram of the network architecture
Details of Finding	there is no network segregation implemented between different departments or user groups. All employees, regardless of their roles and responsibilities, have unrestricted access to the same network and information resources
Impact	Without proper segregation, an unauthorized user may gain access to sensitive data that they shouldn't have permission to access. This can lead to data breaches, loss of intellectual property, or exposure of sensitive customer information If all users and information systems share the same network, a compromise of one system or user account could potentially affect others as well. This can result in the spread of malware, unauthorized modifications to critical systems, or disruption of essential services
Recommandation	Divide the network into different segments based on user groups, departments, or information services. This ensures that each segment has its own network resources and access controls, reducing the risk of unauthorized access or lateral movement within the network Implement appropriate access controls and permissions for each network segment. Use technologies like firewalls, VLANs (Virtual Local Area Networks), or network segmentation appliances to enforce access restrictions between different segments

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	13.2.4 Confidentiality or non-disclosure agreements
How to verify	Review of a sample of confidentiality undertakings or non-disclosure
Proof	sample of confidentiality undertakings or non-disclosure
Details of Finding	not having adequate confidentiality or non-disclosure agreements in place
Impact	The organization may face legal and compliance risks by not having adequate confidentiality or non-disclosure agreements in place. This could result in potential legal disputes, breaches of contractual obligations, or regulatory penalties Without proper NDAs, sensitive information may be at a higher risk of unauthorized disclosure or leakage. This could lead to reputation damage, loss of competitive advantage, or financial harm
Recommandation	Review the organization's information assets and identify the specific needs for confidentiality or non-disclosure agreements. Consider the types of information that require protection, the parties involved, and any legal or regulatory requirements Establish a process to periodically review and update the confidentiality or non-disclosure agreements based on changes in the organization's needs, evolving regulations, or emerging threats. Ensure that the agreements remain relevant and effective in protecting sensitive information

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	15.1.1 Information security policy for supplier relationships
How to verify	Policy review identifying and imposing security measures specific to supplier access to auditee assets
Proof	Policy identifying and imposing security measures specific to supplier access to auditee assets
Details of Finding	the organization does not have a structured framework in place to mitigate the risks associated with the supplier's access to their assets.
Impact	Without clearly defined and documented information security requirements, the organization faces several risks. These risks may include unauthorized access to sensitive data, data breaches, compromised customer information, reputational damage, financial losses, and legal and regulatory consequences.
Recommandation	The organization should engage in a formal agreement or contract with suppliers that clearly states the information security requirements. This agreement should outline the supplier's responsibilities and obligations regarding the protection of the organization's assets

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	16.1.1 Responsibilities and procedures
How to verify	Review of the document defining responsibilities relating to the incident management
Proof	document defining responsibilities relating to the incident management
Details of Finding	there is no established management responsibility or procedure for responding to information security incidents. When a security incident occurs, there is no clear direction or coordination on how to handle the situation. Employees are unsure about whom to report the incident to, how to escalate it, and what actions to take, leading to delays and ineffective response efforts
Impact	Without clear procedures, incident response efforts may be delayed, giving attackers more time to exploit vulnerabilities and causing potential damage to the organization's systems, data, or reputation
Recommandation	Create a dedicated team responsible for managing information security incidents. Define the roles and responsibilities of team members, including incident coordinators, technical experts, and communication liaisons Create a comprehensive plan that outlines the steps to be followed when an incident occurs. Include procedures for incident detection, reporting, assessment, containment, eradication, recovery, and lessons learned Clearly define reporting channels for employees to report security incidents promptly. Establish escalation paths to ensure incidents are escalated to appropriate levels of management and relevant teams based on severity and impact

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	17.1.1 Planning information security continuity
How to verify	Review of business impact analysis report
Proof	business impact analysis report
Details of Finding	there is no documented plan or procedure for managing information security during a crisis or disaster. The organization has not determined its requirements for information security in adverse situations
Impact	During a crisis or disaster, the organization may face severe disruptions and be unable to effectively manage information security. This can lead to data breaches, loss of critical information, prolonged downtime, and reputational damage. The organization may also struggle to recover and resume normal operations in a timely manner
Recommandation	Conduct a thorough business impact analysis (BIA) to identify critical information assets and processes, their dependencies, and the potential impact of their unavailability during a crisis or disaster Develop a comprehensive continuity plan that outlines specific measures and actions to be taken during adverse situations. This plan should include information security considerations and clearly define roles, responsibilities, and communication channels Implement robust backup and recovery procedures to ensure the availability and integrity of critical information. Regularly test and validate the backups to verify their effectiveness

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-037
Auditor	Kanzari
Date and Time	01/01/2023
ISO/IEC Control	18.2.2 Compliance with security policies and standards
How to verify	Review of compliance audit reports
Proof	compliance audit reports
Details of Finding	a manager fails to regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements. They neglect this control and do not perform the necessary reviews
Impact	Without regular compliance reviews, potential security vulnerabilities and weaknesses in information processing and procedures may go unnoticed. This increases the risk of security breaches, data leaks, unauthorized access to sensitive information, or non-compliance with legal and regulatory requirements. The company's reputation could be damaged, customer trust may be lost, and financial losses can occur due to legal penalties or operational disruptions
Recommandation	Establish a documented process that outlines the frequency, scope, and responsibilities for reviewing the compliance of information processing and procedures. This process should clearly define the steps and actions required for managers to fulfill their review obligations