MINISTRY
OF
SECURITY

ISO 27001 AUDIT REPORT TEMPLATE

PRACTICAL SKILLS TO EXECUTE, WRITE A REPORT ON ISMS AUDITS

How to Understand the ISO 27002:2013 Requirements

Master the fundamentals of ISMS audit missions.

Develop practical skills to execute, and report on ISMS audits. Gain

insights into best practices and international standards.

Understand risk assessment methodologies and evaluation techniques.

Learn how to identify vulnerabilities and propose effective recommendations.

IS Audit Report

What is the ISMS Audit Report?

The audit report is a document that provides an assessment of an organization's compliance with the requirements of its information security management system. It evaluates the effectiveness of controls, processes, and procedures in place to protect the organization's information assets. The report identifies non-compliance issues, and provides recommendations for improving the security posture.

Importance of ISMS Audit Report:

The ISMS audit report is crucial for several reasons:

- **Compliance Verification:** The report verifies whether the organization is compliant with applicable standards or frameworks such as ISO 27001

- **Risk Identification and Mitigation:** The report identifies potential security risks and within the organization's information systems. By understanding these risks, the organization can take appropriate measures to mitigate them, reducing the likelihood of security incidents

- **Continuous Improvement:** It helps the organization refine its security controls, processes, and procedures to enhance overall security posture and better protect its assets

- **Stakeholder Confidence:** The report serves as evidence of the organization's commitment to information security. It provides assurance to stakeholders, such as customers, partners, and regulatory bodies, that the organization has implemented appropriate security measures and safeguards

THE SECTIONS OF ISMS AUDIT REPORT:

1. Executive Summary

This section provides a high-level overview of the IS audit findings, conclusions, and recommendations. It is typically written for management or executives who may not have detailed technical knowledge and may not have the time or technical knowledge to review the full audit report.

How to do:

Introduction:

This Executive Summary provides an overview of the findings and recommendations resulting from the recent audit conducted on the Information Security Management System (ISMS) of XYZ Company. The audit aimed to assess the effectiveness and compliance of the company's ISMS with established standards and best practices.

Scope and Objectives:

The audit was conducted between 10/02/2023 and 14/02/2023, encompassing all relevant departments and processes within XYZ Company. The objectives of the audit were to evaluate the implementation, and effectiveness of the ISMS, identify areas of non- compliance, and provide recommendations for improvement.

Audit Findings:

Compliance Assessment: The audit team performed a comprehensive assessment of XYZ Company's ISMS against the relevant industry standards, including ISO/IEC 27001:20XX. Overall, the ISMS demonstrated a good level of compliance, with most controls and procedures aligning with the requirements. However, some areas were identified where improvements are necessary to enhance compliance.

Risk Management: The audit team reviewed the risk management processes in place within the ISMS. While XYZ Company has established a risk management framework, it was observed that the risk assessment methodology needs to be more robust and consistently applied across all departments. Strengthening the risk management practices will contribute to better decision-making and prioritization of security measures.

Access Control: The audit team evaluated the access control mechanisms within XYZ Company's ISMS. Generally, access controls were appropriately implemented, including user authentication, authorization, and privilege management. However, a few instances of inadequate access control configurations were identified, particularly regarding the management of privileged accounts. It is recommended to implement stricter controls and regularly review access privileges to mitigate potential risks.

Incident Response and Business Continuity: XYZ Company demonstrated a well-defined incident response plan and business continuity procedures. However, the audit team observed a lack of periodic testing and updating of these plans. Regular testing, along with the incorporation of lessons learned, is essential to ensure the effectiveness and resilience of the company's incident response and business continuity capabilities.

Recommendations: Based on the audit findings, the following recommendations are provided to improve the effectiveness and compliance of XYZ Company's ISMS:

- Enhance Risk Assessment Methodology: Review and update the risk assessment methodology to ensure consistency across all departments. This includes clear documentation of risk criteria, identification of assets, assessment of threats and vulnerabilities

- Strengthen Access Control Measures: Implement stricter controls for privileged accounts, including regular reviews of access privileges and the implementation of multi-factor authentication for critical systems. Consider implementing a centralized identity and access management system to enhance control and monitoring capabilities.

- Test and Update Incident Response and Business Continuity Plans: Conduct regular testing of incident response and business continuity plans, involving key stakeholders from relevant departments. Incorporate lessons learned from testing and real incidents to update the plans and ensure their effectiveness in handling potential security incidents or disruptions

Conclusion:

In conclusion, the audit of XYZ Company's ISMS highlighted areas of compliance and effectiveness, as well as opportunities for improvement. By implementing the provided recommendations, XYZ Company can enhance its overall security posture, mitigate risks, and strengthen its information security management practices.

2. Audit purpose

This audit refers to the specific objectives or goals that an audit aims to achieve. It encompasses the reasons why an audit is conducted and what it seeks to accomplish.

How to do :

some purposes of isms audit :

- Conducting an audit to assess if the organization's ISMS is compliant with ISO/IEC 27001:20XX, industry-specific regulations (e.g., HIPAA for healthcare), or data protection laws (e.g., GDPR)
- Auditing the organization's incident response procedures to determine if they are efficient in detecting, responding to, and mitigating security incidents effectively
- assess the risks associated with data breaches, unauthorized access, or insider threats, and to evaluate the organization's risk assessment and treatment methodologies
- Auditing the organization's access control mechanisms, such as user authentication, authorization, and segregation of duties, to ensure they are properly implemented and monitored
- Conducting an audit to assess the adequacy and effectiveness of the organization's business continuity plans and disaster recovery processes to ensure they can handle potential disruptions to the ISMS
- Auditing the organization's adherence to its internal information security policies, such as password management, data classification, or incident reporting procedures
- Conducting an audit to assess the security measures and controls implemented by a cloud service provider or a business partner to ensure they meet the organization's security requirements and protect shared data

3. Scope

The scope of an Information Security Management System (ISMS) audit refers to the boundaries and extent of the audit, specifying the areas, processes, systems, and controls that will be assessed during the audit. It defines the limits and coverage of the audit activities and provides guidance on what will be included and excluded from the audit. The scope of an ISMS audit is typically determined based on various factors, such as organizational requirements, audit objectives, regulatory obligations, and risk considerations.

The scope of an ISMS audit may include the following aspects:

Departments and Functions:

The audit scope defines which departments, functions, or business units within the organization will be subject to the audit.

Processes and Systems:

The audit scope identifies the specific processes, systems, or technologies that will be audited. This may include areas such as access control, incident management, network security, data backup

Locations and Facilities:

The audit scope determines the geographical locations or physical facilities that will be included in the audit. This is particularly relevant for organizations with multiple offices, data centers, or branches. The scope may encompass specific locations or have a global coverage, depending on the organization's needs.

Standards and Frameworks:

The audit scope outlines the specific standards, frameworks, or best practices against which the ISMS will be audited

Exclusions:

The audit scope may explicitly state any areas, functions, or processes that are specifically excluded from the audit. This could be due to practical constraints, limited resources

How to do:

- ***Departments and Functions:***

  The audit will encompass all departments and functions within XYZ Corporation, including but not limited to IT, Human Resources, Finance, Operations, and Legal.

- ***Processes and Systems:***

  The audit will focus on the following key processes and systems within XYZ Corporation's ISMS:

  a. Access control and user management

  b. Incident management and response

  c. Network and infrastructure security

  d. Data backup and recovery

  e. Vendor and supplier management

  f. Employee awareness and training programs

- ***Locations and Facilities:***

  The audit will cover all physical locations and facilities operated by XYZ Corporation, including head office, regional offices, and data centers

- ***Standards and Frameworks:***

  The audit will be conducted in accordance with the requirements of ISO/IEC 27001:20XX standard for Information Security Management Systems

- ***Exclusions:***

  The following areas are explicitly excluded from the scope of this audit: a. Physical security of non-IT assets, as this falls under a separate physical security audit. b. Compliance with specific industry regulations, such as healthcare regulations or financial sector-specific requirements, as those are subject to separate audits

4. Categorization of audit findings

Audit findings are the results or outcomes of an audit. They represent the auditor's assessment and evaluation of the audited entity's compliance or non- compliance with specific criteria, such as regulations, standards, policies, or best practices.

The audit findings are classified as below:

Non-Conformity: Non-conformity refers to a finding where an organization's practices, processes, or controls do not meet the required standards. It indicates a significant deviation from the expected or desired state and represents a failure to comply with specific requirements

Observation: An observation is a finding that highlights an area for improvement or a best practice suggestion. Unlike a non-conformity, an observation does not indicate a failure to meet a requirement or standard but rather provides recommendations for enhancing the organization's processes, controls, or practices

Conformity: Conformity findings indicate that the audited practices, processes, or controls align with the prescribed standards, requirements, or criteria. These findings signify that the organization is successfully meeting the expected level of compliance

5. Audit Sampling How to do :

Item	Details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-01
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	IS Policy
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
Recommendation	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-02
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	Official designation of different IT responsibilities
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
Recommendation	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-03
Date and Time	01/01/2023
ISO/IEC Control	6.1.2 Segregation of duties
How to verify	° Review of job description ° verification of access rights
Proof	Job description
Details of Finding	The organization has not implemented effective segregation of duties within the finance department. The same individuals have been assigned both authorization and custodial responsibilities Some individuals having the ability to initiate and approve financial transactions without appropriate checks and balances
Impact	Fraudulent activities, such as unauthorized payments Without adequate separation, there is a higher likelihood of errors or unintentional mistakes in financial transactions, leading to inaccuracies in financial records, improper reporting, or misallocation of funds
Recommendation	Conduct a thorough review of the finance department's roles and responsibilities. Clearly define distinct roles such as initiator, approver, and custodian for financial transactions. Ensure that no individual has complete control over the end-to-end financial process Updated policies and procedures that clearly outline the segregation of duties requirements within the finance department

Item	Details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-04
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
Recommendation	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-05
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
Recommendation	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-06
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
Recommendation	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-07
Date and Time	01/01/2023
ISO/IEC Control	6.2.2 Teleworking
How to verify	Review of the policy on the use of telework
Proof	the policy on the use of telework
Details of Finding	The organization does not have a policy in place to protect information accessed, processed, or stored at teleworking sites. There are no specific security measures or guidelines provided to employees working remotely
Impact	The lack of a policy and security measures for teleworking sites increases the risk of unauthorized access, data breaches, and information leakage. Confidential information could be compromised, leading to reputational damage, regulatory non-compliance, and financial losses
Recommendation	Develops and implements a comprehensive teleworking policy along with supporting security measures. The policy should outline guidelines for secure remote access, data protection requirements, and the use of encrypted communication channels. Security measures may include the use of virtual private networks (VPNs), two-factor authentication, endpoint protection, and data encryption. Regular employee awareness and training programs should also be conducted to ensure adherence to the policy and promote secure teleworking practices

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-08
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
Recommendation	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-09
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
Recommendation	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-010
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
Recommendation	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-011
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
Recommendation	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-012
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
Recommendation	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-013
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
Recommendation	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-014
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
Recommendation	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-015
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
Recommendation	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-016
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
Recommendation	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-017
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
Recommendation	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-018
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
Recommendation	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-019
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
Recommendation	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-020
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
Recommendation	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-021
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
Recommendation	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-022
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 is 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
Recommendation	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

item	details
Type of Finding	Non-conformity (NC)/major
Finding ID	NC-023
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.
Recommendation	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

Type of Finding	Non-conformity (NC)/major
Finding ID	NC-024
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
Recommendation	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-025
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
Recommendation	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-026
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
Recommendation	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-027
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
Recommendation	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-028
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
Recommendation	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-029
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
Recommendation	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-030
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
Recommendation	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	NC-031
Date and Time	01/01/2023
ISO/IEC Control	9.3.1 Use of secret authentication information
How to verify	Review of awareness session programs
Proof	awareness session programs
Details of Finding	employees might use weak passwords or share their authentication credentials with unauthorized individuals
Impact	Weak passwords and sharing authentication credentials can lead to unauthorized users gaining access to critical resources, data breaches, loss of confidentiality, and potential financial and reputational damage to the organization.
Recommendation	Define and communicate clear guidelines for creating strong and unique passwords. Encourage the use of multifactor authentication (MFA) to enhance security Conduct regular awareness programs and training sessions to educate employees about the importance of following authentication practices

Type of Finding	Non-conformity (NC)/major
Finding ID	NC-032
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
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
Recommendation	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-033
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	logs
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
Recommendation	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	NC-034
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 creatingstrong 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
Recommendation	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

Type of Finding	Non-conformity (NC)/major
Finding ID	NC-035
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
Recommendation	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
	Author: Noureddine Kanzari **Published by Ministry of Security**