Sri Lanka Institute of Information technology

2024

Enterprise Standards for Information Security – IE3102

Year 3, Semester 1

Report on ISO 27001:2022(ISMS) Implementation for an Organization (e.g., small business, healthcare, financial institution)

❖ Group Members

Gunasekara A.G.M. K	IT22587138	it22587138@my.sliit.lk	0769755940
Pathirana P.S. S	IT22181510	it22181510@my.sliit.lk	0773928469
Thilakarathna P.L.B.H	IT22567642	it22567642@my.sliit.lk	0776597112
Dushmantha I.W.A. R	IT22572974	it22572974@my.sliit.lk	0765421476
Jayarathna K.P.G.C.M	IT22562074	it22562074@my.sliit.lk	0769994184

Table of Contents

Introduction

Purpose of the Report

It is also important to note that the purpose of preparing this report is to present a strategy that will help to carry out the Information Security Management System in line with ISO 27001:2022 in HNB Finance. As the aim is to assist the organization in ensuring compliance with ISO 27001:2022: managing information security risks affecting an organization's information assets, the following report attempts to provide recommendations. Such a program will help to provide a step-by-step plan for developing effective ISMS that would address legal requirements and organizational goals.

Further, it is the mandate of the report to analyze probable threats facing the organization's information and specify the sound policies, procedures, and controls for managing the threats. It also describes authorities and responsibility of main persons and teams that are participating in the process of implementation of the ISMS. It will also provide a way for guaranteeing the constant enhancement of the ISMS and promoting an employee security-consciousness.

What is ISO 27001:2022?

ISO 27001:2022 is an ISMS standard which has gained international acceptance in organizations seeking to manage their information security. People, processes, and technology are employed to safeguard information in an organization in the context of access, usage, disclosure, availability, alterability and destroy ability or loss. An objective of the standard is to fit into the overall family of standards ISO/IEC 27000 that is used to direct organizations on managing information security risks with the aim of enhancing the security, confidentiality, integrity and accessibility of information.

ISO 27001:2022 lays down the specifications of an organization's ISMS in the context of the said organization's broader risk environment. ISMS offers a structure composed of the policies, procedure and or any other control that must be in place to safeguard the information asset and or manage risks affecting those assets.

Why is ISO 27001:2022 Important?

ISO 27001:2022 holds significance for several reasons, which are still valid in the present world that is more digitally exposed than ever was. Key reasons for its importance include:

- Regulatory Compliance:
  - Currently there are a few industries and facilities where information security and data protection are currently heavily regulated such as healthcare industry, finance industry as well as life science industry. The contextualized information security instruction made available through ISO 27001:2022 is valuable in addressing specific data protection regulations like the GDPR, NIS regulations and other local and other international laws.
- Risk Management:
  - It provides guidelines of aspects that can be risky to an organization’s information assets hence facilitating their assessment in a bid to prevent potential losses. The mitigation approach enables organizations to deal with the threats as they come along before they get exploited by the cyber attackers.
- Developing Stakeholder Trust:
  - One of the significant factors for an organization is Information security and certification under ISO 27001 informs partners, consumers and other stakeholders of this fact. In business relations it enhances confidence as demonstrated in the case of the organization adopting measures to enhance data security in business relations.
- Cyber Threat Protection:
  - When it comes to protection against risks and their related threats and attacks, ISO 27001 provides a very wide number of choices for dealing with internal and external threats and with attacks such as phishing, hacking, internal threats and inadvertent data disclosure. It reduces a company’s probability of costly breaches and data loss events by helping them safeguard their information resources.
- Alignment with Business Goals:
  - The standard ensures that the management of information security aligns to the general strategic direction of an organization. The core of ISO 27001 ensures that security because it hinders every step assists rather than hinders business goals of the organization by integrating security controls into the business processes.

What are the Benefits of ISO 27001:2022?

Implementing ISO 27001:2022 offers several benefits to organizations across various sectors:

- Better Security Posture:
  - It will help in developing a suitable security structure with the controls, policy and overall protection mechanisms with the help of ISO 27001:2022 information assets and thereby protect the firms. And so, the development of improved security measures against cyber threats, data leakage, and other security threats are the result
- Improved Risk Management:
  - Organizations must create risk treatment plans and carry out routine risk assessments in accordance with the standard. By continuously assessing and managing risks, the company makes sure that its security plan stays in line with its goals and changes to counter new threats
- Competitive Advantage:
  - Being certified in accordance with ISO 27001 can act as distinct competitive advantage. In industries that are most sensitive and controlled, say the financial sector, healthcare or the life-sciences, it is a major selling point to reassure the clients and partners that the company would like to keep their information safe.
- Reduced Complexity in Compliance:
  - Adoption of the ISO 27001 standard can be convenient in ensuring that the organization complies with other standards and laws. Organizations which obtain a certification to ISO 27001 can more effectively prove compliance to numerous regulations and align other ISO regulations' compliance.
- Efficiency in Operations and Ongoing Improvement:
  - By mandating frequent evaluations, audits, and ISMS updates, the standard fosters an environment of ongoing improvement. Through this continuous process, organizations can improve their security controls, lower the cost of data breaches, and guarantee that security will always be effective and efficient

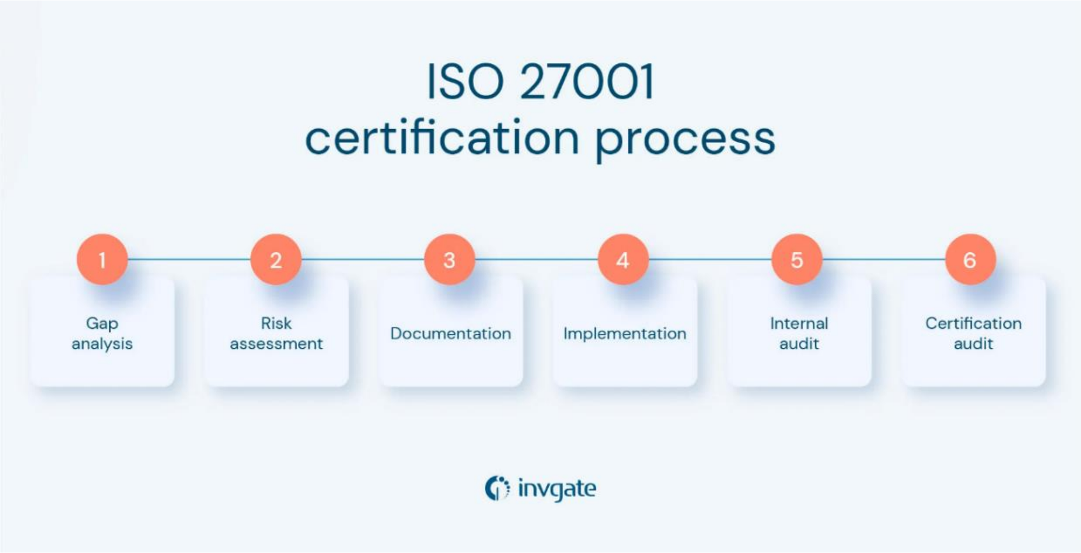
How to Implement ISO 27001:2022 Certification?

- Prepare:
  - Purchase the ISO 27001:2022 standard and read it to at least gain some knowledge on what it says.
  - Make sure that the top management of the organization is fully involved in the support for the project since it is important.
  - Conduct a gap analysis to see how current measures compliant with ISO 27001 standard.
- Establish the Scope, Context, and Objectives:
  - Determine the extent of ISMS in relation to its internal and external environment and it stakeholders as well as their expectations.
  - Use a PESTLE analysis to know the degree of impact that political, economic, sociological, technological, legal and environmental factors have.
  - Develop organizational information security goals and determine how they could be met, making sure they are written down, shared and then checked.
- Establish a Management Framework:
  - Develop a management framework that outlines the processes to achieve your objectives. This includes a schedule of activities, accountability for the ISMS and regular auditing to support continual improvement
- Conduct a Risk Assessment:
  - Conduct a risk analysis, assessment and evaluation to ascertain risks in the company. ISO 27001 states that an appropriate risk assessment process has to be implemented which generates valid, consistent and comparable risk assessment results.
- Implement Controls to Mitigate Risks:
  - Decide how to address identified risks using one of the four options: modify (implement a control), avoid (stop the source of the risk), share (outsource) or retain (accept the risk)
  - Document all risk-related decisions and create a Statement of Applicability (SoA) and a risk treatment plan
- Conduct Training:
  - Ensure all staff are aware of the ISMS, its benefits, the information security policy and the implications of not meeting ISMS requirements
  - Conduct training for staff to ensure competence in maintaining and operating the ISMS

- Review and Update Required Documentation:
    - Ensure all required documentation is created and maintained, as stipulated by ISO 27001 and necessary for the ISMS to function effectively. Core documents like the SoA and risk treatment plan must be produced
- Measure, Monitor, and Review:
    - Continually measure and monitor the ISMS's performance against its objectives to identify areas for improvement. Continual improvement may involve reducing costs or achieving better results with the same investment
- Conduct an Internal Audit:
    - Conduct frequent internal assessments with a view of ascertaining that the organization’s ISMS meets with ISO 27001 standard and is efficient. Create an efficient audit schedule that would cater for all ISMS standard and other organizational demands for the program.
- Certification Audits:
    - Undergo a certification audit conducted by an accredited external certification body. The process is in two stages:

        Stage 1: Preliminary review to ensure the ISMS is implemented correctly

        Stage 2: Detailed assessment of the ISMS's effectiveness and compliance with ISO 27001 requirements



What are ISMS?

An ISMS is a formal system which aims to safeguard the information of an organization and its possession, content, and accessibility. Therefore, it aligns processes, technologies and resources to enable proper management of information security risks. ISMS requires formulation of policies, procedures and controls particular to an organization that will adhere to ISO/IEC 27001, the international Standard for implementing ISMS.

In its deepest form, an ISMS protects information assets from compromise through unauthorized access, disclosure, alteration or destruction through vast risk assessments to inform the right choice and setting of proper security measures. Such an approach is beneficial in developing a security-aware culture of the organization’s employees and following the legal requirements regarding data protection and preventing any breaches and cyber incidents.

Implementation of an ISMS allows the organization to maintain information security in the most effectively coordinated and flexible way possible and minimize the risks of security breaches, increase stakeholders’ trust as well as prove compliance with the globally accepted standards for managing information security.

What are the Benefits of ISMS?

- Data Protection:
  - An ISMS helps to maintain protection of the information from the external environment, invasion, break-ins and hackers. It means that through adopting proper control and security measures, different organizations can safeguard important information including customer details, intellectual capital and other financial details.
- Risk Management:
  - Effective risk management is a core component of an ISMS. It is a process of evaluating the risks that would affect information security and the measures that can be taken to avoid them. In this way organizations can prevent or at least minimize the risks and impacts of security threats and risks.
- Regulatory Compliance:
  - An ISMS helps organizations to adhere to industry regulations, standards and legal requirements, such as GDPR, HIPAA or PCI DSS. Observance of these regulations is crucial in ensuring that organizations do not land in hot water with the law as well as showing commitment toward the safeguarding of the information.
- Business Continuity:
  - An ISMS also has disaster recovery and incident response plans that enable a speedy recovery from any security incident, also avoiding disruptions of business. They assist organizations to develop mechanisms of handling possible cybers threats.
- Improved Reputation and Stakeholder Trust:
  - An organization that implements an ISMS has the benefits of showing a good stand in the security of information. These help in building confidence among the customers, partners and even investors.

Overview Of HNB Finance

HNB Finance PLC is among the top financial service providers in Sri Lanka, which began operating in the year 2000 as a subsidiary of Hatton National Bank, a prominent commercial bank in the country. The organization has grown significantly over the years and has become a trusted name in the financial sector

Size and Reach

- HNB Finance employ over 70 branches and service centers all over Sri Lanka. This extensive presence enables it to serve a diverse customer base, including individuals, small and medium-sized enterprises (SMEs) and larger corporations.

Business Functions

- Retail and Corporate Banking: HNB Finance offers services including savings accounts, fixed deposits and business loans and other retail and commercial banking products.
- Lending: The organization offers different kinds of loans including personal, business, home loans and leasing services to meet various consumers' demands.
- Leasing: Vehicle and machinery leasing services are among HNB Finance key offers targeting both individuals and companies.
- Microfinance: HNB Finance's microfinance service empowers the small-business segment by providing credit and financial products to start-ups and existing businesses.
- Digital Banking Solutions: The firm targets the operationalization of a digital platform to improve clients' satisfaction and develop the service provision through mobile and internet banking.

Market Presence

- With a solid financial foundation, good and efficient governance structure and being closer to the customer needs HNB Finance has set itself a place in Sri Lanka as a competitive and trusted financial company. It has been able to sustain growth through diversification of products, clients and market with the implementation of new ideas.

Regulatory Environment

- HNB Finance as a financial services company in Sri Lanka operates under the regulations of the Central Bank of Sri Lanka (CBSL). This entails compliance with several regulatory requirements in the financial, operational, and information security domains such as money laundering and Know-Your-Customer (KYC) standards.

Scope Of the ISMS

Objective

To identify and specify the scope as well as the extent of the application of the Information Security Management System within HNB Finance, as well as its relationship with business strategies, legal demands and risk management frameworks.

ISMS Scope Statement

The scope of the ISMS for HNB Finance covers all critical departments, functions, processes, and information systems that manage, process, or store sensitive financial and personal data**.**

Included Departments

- Information Technology (IT) Department:

  Responsible for the management of IT infrastructure, cybersecurity, and data management systems.

- Operations Department:

  Manages day-to-day transactions, customer service platforms, and business continuity.

- Customer Service Division:

  Handles customer interactions and data through various channels, including call centers and digital platforms.

- Risk Management and Compliance Department:

  Monitors regulatory compliance, risk management, and information security controls.

- Digital Banking Division:

Manages online banking, mobile applications, and related digital services.

Internal Audit Department: Responsible for auditing ISMS processes and controls.

- Finance and Accounting Department:

  Processes financial data and is involved in transaction verification and fraud detection.

Functions And Processes

- Customer Data Management:

  Systems and processes used for storing, managing, and processing customer financial and personal data.

- Digital Transactions and Payments:

  Systems supporting online transactions, digital wallets (e.g., HNB SOLO), and payment gateways.

- Cybersecurity Management:

  All controls related to network security, application security, incident response, and vulnerability management.

- Risk Management and Compliance Monitoring:

  Continuous monitoring and management of financial and non-financial risks, including regulatory compliance.

- Business Continuity and Disaster Recovery:

  Ensuring systems and processes remain operational during and after a disruptive event.

Included Information Systems

- Core Banking Systems:

  Platforms managing all banking transactions and account management.

- Customer Relationship Management (CRM) Systems:

  Platforms used for managing customer interactions and data.

- Digital Banking Platforms:

  Systems for online banking, mobile banking applications, and digital wallets.

- Data Warehouses and Reporting Systems:

  Systems used for data storage, analysis, and reporting, particularly related to customer data and transactions.

- Internal Network and Communication Systems:

  Systems that manage internal communications, data flow, and network security.

Non – Critical administrative Functions

- Human Resources
- Marketing
- Facilities Management are excluded from the ISMS scope

Third – Party vendor System Not Integrated

- External systems and third-party vendor platforms not integrated with HNB Finance's internal systems are excluded. However, data exchanged with these vendors must still comply with data protection and security requirements outlined by the ISMS.

Justification Of Scope

- The scope defined to align with HNB Finance's Business Objectives, Regulatory Environment and Risk Management

Business Objectives

- HNB Finance prioritizes customer trust and uninterrupted service by securing customer data, transactions, and digital platforms.

Regulatory Environment

- Compliance with the Central Bank of Sri Lanka's regulations, including anti-money laundering and KYC standards, necessitates a comprehensive ISMS for all sensitive data and transaction systems.

Risk Management

- Risk management efforts are increasingly concentrating on systems and procedures—like online banking and digital wallets—that are particularly susceptible to cyberattacks and digital transformation projects.

Roles and Responsibilities

1. Project Manager

- Responsibilities:
  - Oversees the overall ISMS implementation project, specifically for its timeframe and costs.
  - Maintains the project plan as well as the definition of the key milestones, the timeline and deliverables.
  - Defines the roles of each person in relation to others and organize the work of all individuals in a group.
  - Manages resources, including human, financial, and technological, required for the successful functioning of the ISMS.
  - Enables interaction with a variety of different stakeholders, such as the Board of Directors, the Organization’s top executives and the personnel in charge of implementing the ISMS.
  - Creates consistent reports to the Board Integrated Risk Management Committee (BIRMC) on the state of the ISMS with focus on the challenges, risks and decisions encountered.

2. Risk Assessment Lead

- Responsibilities:
    - Identifies and assesses risks of harm to HNB Finance’s information assets under the general risk management environment.
    - Performs detailed risk analyses utilizing tools and approaches like risk profiles, risks assessment charts and effect analysis.
    - Carries out risk assessment workshops with key stakeholders to discuss and evaluate potential threats and vulnerabilities.
    - Preparing of the risk assessment report including identified sources of risk, the vulnerability of the organization to those sources and recommended measures to be taken to eliminate these sources of risk.
    - Engages the Chief Risk Officer (CRO), and other personnel within the risk management division to ascertain that the risk assessments done within the framework of the ISMS are in harmony with the Bank’s risk tolerance and guidelines.

3. ISMS Policy and Procedure Developer

- Responsibilities:
    - Develops ISMS policies and supporting procedures consistent with ISO 27001:2022 and HNB Finance’s existing governance frameworks.
    - Oversees the accuracy and compliance of all the ISMS policies at HNB Finance including data protection policy as well as access control policy.
    - Consults with stakeholders, including department heads, legal advisors, and the Board, for the approval of policies as required.
    - Constantly reviewing and updating the organization’s ISMS policies, regulatory requirements that have been released by Central Bank of Sri Lanka, and Payment Card Industry Data Security Standards (PCIDSS).
    - Works hand in hand with the compliance and legal departments to properly communicate and enforce organizational policies.

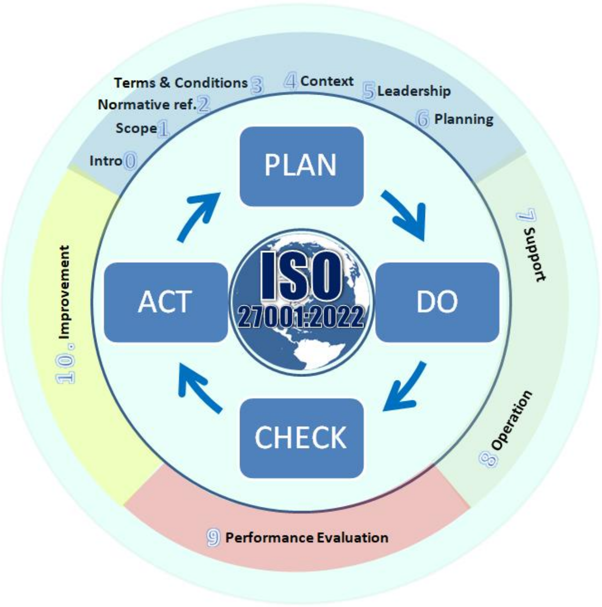
4. Implementation and Compliance Officer

- Responsibilities:
  - Supervises the execution of the ISMS controls, guaranteeing sufficient deployment into the concept of the ISMS as well as the risk treatment plan.
  - Ensures that the operations of the organization adhere to the general ISO 27001:2022 standards and some specific laws like the Banking Act as well as some internal corporate governance policies.
  - Carries out internal audits and assessments that help it determine the efficiency of the ISMS control and the possible risks that may exist within the organization.
  - Ensures that all documented records including audit reports, checklists for the compliance assessments and/or other corrective action plans concerning the ISO 27001 and other regulatory policies are developed and retained.
  - Delivers compliance report to the Board Audit Committee (BAC) and the BIRMC on scheduled time intervals with information about the implementation of the ISMS and non-compliance incidents.

5. Security Awareness and Training Coordinator

- Responsibilities:
  - Implement an organizational wide program on Security Awareness and Training tailored to different roles within HNB Finance.
  - Develops learning resources and facilitates training sessions covering topics such as cybersecurity awareness, data privacy, incident response and regulatory compliance.
  - Works closely with the Human Resources and IT departments to guarantee compliance of the training programs with the Bank’s policies and new security risks.
  - Evaluates outcomes of the training program by using assessments, feedback and monitoring of associated incidents to have better standards.
  - Ensures the training material is reviewed and changed from time to time with new threats, new regulations in information security and improved practice.

ISMS Policy



Objective

The purpose of the ISMS policy is to review and outline the aim, extent and commitment from the management at HNB Finance for the creation of a secure framework in the management of information at the firm. The next policy presents goals, roles, responsibilities, procedures necessary to ensure legal, regulatory and contractual compliance for safeguarding information assets.

- Protecting Customer Data:

  Make it possible to prevent all customer data from being accessed, changed and lost by a third party. This includes actions such as data encryption, controlling the access to the data, safe storage of the data among others.

- Ensuring Business Continuity:

  Implement a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for the enterprise and/or business units to ensure availability of vital functions and limit the adverse effects of Information Security incidents.

- Compliance with Regulatory and Legal Requirements:

  Comply with the Central Bank of Sri Lanka regulations, the GDPR and the Payment Card Industry Data Security Standard (PCIDSS).

- Risk Management:

  Manage risk to information security through conduct of risk assessment, vulnerability assessment and penetration testing.

- Promoting Security Awareness:

  Improve the level of awareness of all personnel and stakeholders concerning information security through regular training, workshops and communication initiatives.

Policy Statement

Regarding information security risks management, HNB Finance has a definite mission of safeguarding all its information resources from all risks regardless of being internal or external, deliberate or accidental. The organization has recognized that information security is crucial for protecting the customer’s confidence, achieving business responsiveness and satisfying the legal, regulations and contractual requirements. This document provides guidelines of how to very effectively implement and manage the strongest ISMS to conform to the ISO 27001:2022 and to ensure the confidentiality, integrity and availability of information.

Key commitments of the ISMS policy include

- Preserving the confidentiality, integrity and availability of all forms of information.
- Implementation and compliance with all rules and regulations Such as the Central Bank of Sri Lanka rules & Regulations GDPR & PCIDSS etc.
- Present reporting of hazard identification and implementation of relevant risk control measures for information security risks.
- Maintaining an organizational focus on information security and the constant practise of being vigilant.

Principles

- Confidentiality: To make certain that only authorized persons can access and retrieve confidential information, and that this information is protected from disclosure.
- Integrity: Ensuring data integrity and maintaining compliance of data and the methods for processing, specifically controlling against data alteration or deletion without proper authorization.
- Availability: The process of making sure that information and the assets related to it can be readily available and subsequently used by the people who are allowed to use it whenever there is a need to do so.
- Accountability: Ensuring that there is always clear responsibility and reporting of information security management at organizational hierarchy.
- Continuous Improvement: Continual improvement and checking/ updating of the ISMS in relation to threats, changes in business and new technologies.
    - controlled in conjunction with other types of risks such as credit risks, market risks, operational risks among others that may prevail in an organization.
    - The policy requires constant risk assessments to determine the risks in securing information and putting measures to manage them and the results will be forwarded to the CRO and the Risk Management Committee.
- Alignment with Strategic Business Objectives:
    - The purpose of ISMS policy is to align with the existing HNB Finance strategic directions like digitalization, customers' satisfaction and organizational reliability. For instance, strategies on data protection and security policy are consistent with the bank's strategy on improving customer satisfaction and their data security, especially in different digital hubs such as online banking and mobile apps.

Integration with Other Policies and Procedures

- Privacy and Data Protection Policy Integration:
    - The ISMS policy is very much aligned with the existing Privacy and Data Protection policy of HNB Finance. Consequently, it states the procedures of working with personal data in accordance with the GDPR and the regulations of data protection in Sri Lanka. This entails coming up with guidelines on how to collect, process, store and dispose of data.
    - Other individual controls include information security management GM strategy ISMS for data privacy like encryption of data, implementation of the protection of passage to the data, data protection techniques such as data loss prevention (DLP).

- Incident Management and Response Procedures:
    - The ISMS policy encompasses an Incident Management Policy in as far as the identification, reporting, management and even the recovery process of Information Security incidents are concerned. This includes detailed steps for incident detection, escalation, analysis, containment, eradication, and post-incident review.
    - This policy requires formation of the incident response teams, training of the teams as well as the conduct of the incident response exercises [e.g. Tabletop exercising].
- Third-Party Risk Management:
    - The ISMS policy covers the third-party vendors and partners to maintain the same level of security compliance as HNB Finance. This includes carrying out third party risk management, setting legal acreage regarding information security and third-party monitoring.
    - There are certain clauses that are implemented in vendor contracts so that they follow the security standards recommended and depending on the circumstances there are possibilities of executing audits/assessments conducted by HNB Finance

Practical Examples of ISMS Controls and Implementation

- Access Control Management:
    - The ISMS policy includes the restricted access of the information and the systems containing such information in that only authorized persons are permitted to access the information. This entails Role-Based Access Control (RBAC), Multi-factor authentication (MFA) and Access reviews, done at certain intervals.
    - Access controls work with User Identity and Access Management (IAM) systems so as to automate the ways of managing or granting rights to users.
- Data Encryption and Cryptographic Controls:
    - The policy requires that protected data should be encrypted when in transit and when stored in a system either offline or online. This includes encryption algorithms that are very hard to crack and other matters that should ensure key management to minimize cases of data leakage.
    - Encryption is carried out in the case of data transmission, communication and storage to ensure data integrity and data security.

- Physical Security Controls:
    - The ISMS policy outlines measures to be adopted in implementing physical security measures of information assets. This will comprise of physical security at data centers, surveillance systems, facility environment such as temperature and humidity, and power resources backup systems.
    - The policy mandates the periodic evaluation and review of physical security controls to check their relevancy in mitigation of risks.
- Network Security and Monitoring:
    - The policy defines measures that are to be taken regarding network security controls including firewalls, IDPS, segmentation of the network and remote access among others. These controls are critical in the prevention of cyber security threats to the organizations' network systems.
    - Continuous network monitoring is conducted to identify emerging or emerging signs of improper activity, attempts at unauthorized access, and threats.

Training and Awareness Programs

- Role-Based Security Training:
    - According to the ISMS policy, every employee is required to undergo training at periodic intervals depending on their work content. These are IT and security personnel training, general employee training and training based on identified high-risk positions.
    - Training programs are updated periodically with the result that new threats, new vulnerabilities, and new regulations are incorporated. To ensure that they understand the concept and are ready to adopt the change, employees undergo tests that include assessments, simulations etc.
- Leadership and Executive Engagement:
    - The policy focuses on the role of leadership and executives in enhancing security awareness and practices within the business environment. This contains a process of periodic presentation of a brief to the Board and the senior management on the trends, risks in security as well as the progress of implementing ISMS.
    - Executives also take part in the development of incident responses drills and tabletops to make sure they are well-prepared for decision making during security incidents.

Approval and Communication

- Policy Approval:

  The ISMS policy shall be endorsed by the Board of Directors to reflect the strategic directions and objectives of the organization as well as compliance to the regulatory standards. The approval process includes receiving and supporting by the Board Integrated Risk Management Committee (BIRMC), the Board Audit Committee (BAC) and other significant governance bodies.

- Policy Communication:

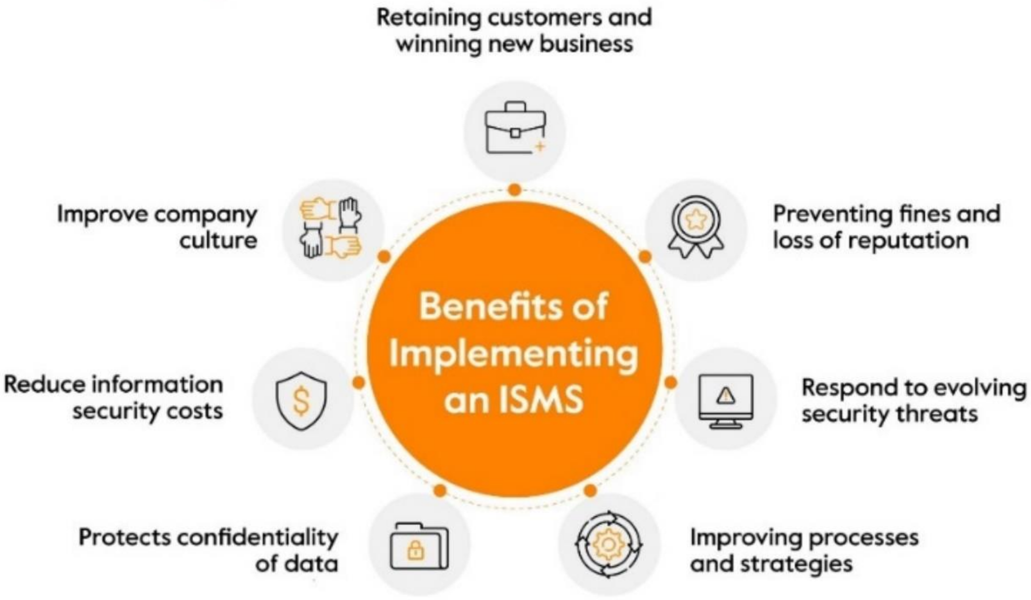
  Upon the approval of the ISMS policy, its implementation will entail disseminating the policy to all the organization's employees, contractors, and all other third parties. Communication methods include:

  - Displaying the policy on the organization's internal website and on the organization's, public facing web site.
  - This includes the provision of training and workshops on the policy and duties and responsibilities of the employees.
  - Offer the related ISMS policy as a part of new employees' orientation and as a part of the annual refresher training.
  - Issuing regular communications through internal newsletters, emails, and bulletin boards to reinforce key policy points and updates.

Policy Review and Continuous Improvement

- Periodic Policy Review Cycle:
  - The ISMS policy provides criteria for a proactive periodic review, which may be annual or more often in the event of updates in the legal requirements and the enterprise's activities and risks. The review process is done by the Information Security Manager together with CRO and with the assistance of the Internal Audit team.
  - In the course of the work, inputs from the department heads, the employees, external auditors, and the regulatory bodies are sought to ensure coverage of all risks and compliance tests anticipated.
- Feedback Mechanisms and Policy Updates:
  - A feedback process is incorporated in the policy to enable the employees and stakeholders to contribute their opinion on the improvements that need to be made on the ISMS. Such feedback is incorporated in the review process so as to give the policy the latest information and the most updated information.

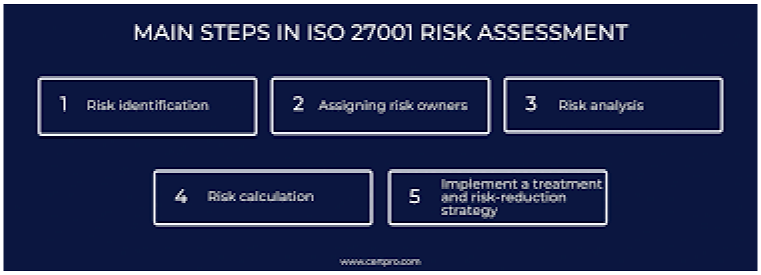
- Other changes made in the ISMS policy are also shared with the employees through internal mechanisms such as newsletters, training sessions, or notices on the company intranet so that they can know about these changes as well as some of the possible repercussions.


Retaining customers and winning new business
Improve company culture
Preventing fines and loss of reputation
Benefits of Implementing an ISMS
Reduce information security costs
Respond to evolving security threats
Protects confidentiality of data
Improving processes and strategies

Risk Assessment Report

Risk Assessment Plan is a formal documented procedure whereby an organization defines the steps and activities which will help it in recognizing, assessing, evaluating as well as controlling risks. It becomes the guide for carrying out assessments of risks to determine and come up with measures to counter threats to an organization's assets, operations and goals.

In the instance of an organization such as HNB Finance it would be imperative to have a Risk Assessment Plan that would be useful in addressing issues such as protection of the financial data, legal compliancy and business sustenance.



MAIN STEPS IN ISO 27001 RISK ASSESSMENT

1 Risk identification

2 Assigning risk owners

3 Risk analysis

4 Risk calculation

5 Implement a treatment and risk-reduction strategy

www.certpro.com

Methodology

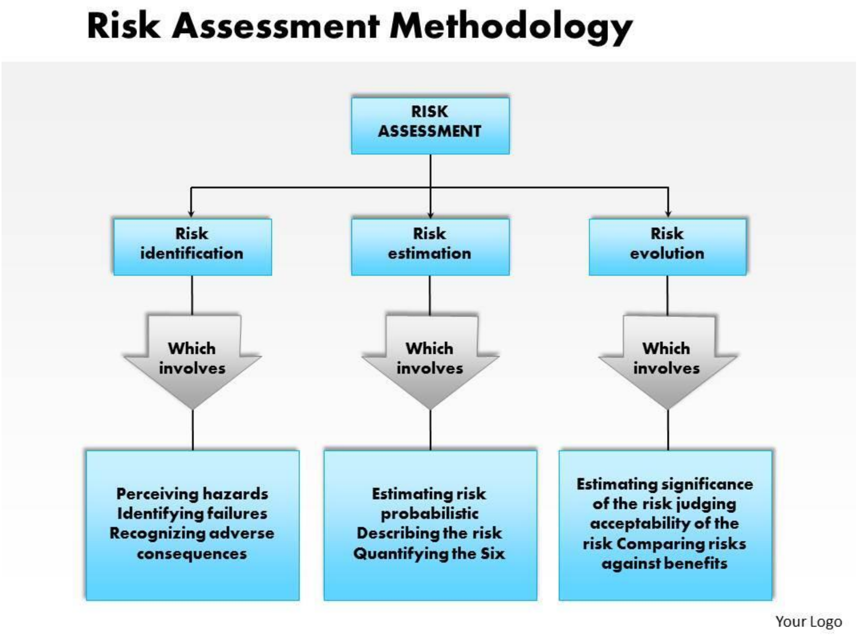
Choose a Risk Assessment Methodology: For this report it is possible to use concepts that correspond to methodologies like ISO 27005, NIST SP 800-30 or FAIR. Here's a brief overview of each:

- ISO 27005:

  This standard offers guidance on the management of information security risk which involves the identification of risk, the assessment of risk and finally risk treatment. It focuses on the systematic procedure of addressing information security risks.

- NIST SP 800-30:

  The following is a PROCEDURE that shows how risk management is carried out comprising of risk identification, risk assessment, risk response and monitoring. It is most helpful to risk identification and risk evaluation to some extent.



Risk Assessment Methodology

RISK ASSESSMENT

Risk identification

Risk estimation

Risk evolution

Which involves

Which involves

Which involves

Perceiving hazards Identifying failures Recognizing adverse consequences

Estimating risk probabilistic Describing the risk Quantifying the Six

Estimating significance of the risk judging acceptability of the risk Comparing risks against benefits

Your Logo

Risk Identification

Assets Identification: Enumerate all the objects that fall under the scope of the program these include databases, servers, customer’s information, applications and human assets.

Threat Identification: Consider possible threats which can endanger these assets as for example cyber threat, malicious insider, virus/malware, natural disasters, operational mistakes.

Vulnerability Identification: Label elements of a system that may be susceptible to threats, for instance, open vulnerabilities, unimplemented software updates, poor user authentication, no encryption, or poorly organized backup mechanisms

Risk Analysis

- Likelihood Assessment: Given below is a step-by-step guide to assess how likely each threat is to take advantage of each vulnerability. It can be done in relative terms for instance, low, medium or high or in terms of numbers for instance percentage and frequency.
- Impact Assessment: Assess the likely losses or the loss that may be incurred from a risk event in terms of the organization’s tangible and intangible assets, productivity, profitability and reputation.

Risk Evaluation

- Risk Rating and Prioritization: When figuring out the levels of risk switch between a risk matrix or scoring system to evaluate the chances of an event occurring alongside its likely impact. (Low, Medium, High)
- Risk Appetite: Decide which risks are tolerable according to the organization's risk tolerance and which ones first need action to be taken.

Risk Treatment

- Mitigation Strategies: Apply firewalls or perform security checks regularly, improve the employee's awareness on security or use authentication measures such as two factor authentication.
- Risk Acceptance: Decide if some risks can be accepted without further action.
- Risk Avoidance: Determine if any risks can be avoided by changing processes or discontinuing certain activities.
- Risk Transfer: Take some risks away from your business and delegate them to other parties, for instance obtain insurance or hire a service provider.

Monitoring and Review

- Design a procedure on how to observe the risks and the achievement of the controls that have been put in place.
- Design a procedure on how to observe the risks and the achievement of the controls that have been put in place.

Documentation and Reporting

- Ensure proper documentation of the risk assessment process, the risk identification and evaluation process and the risk treatment process.
- Present the findings to the senior management and other stakeholders so that the necessary decisions and resources can be made accordingly.

Risk Treatment Plan

In the case of risk treatment, a document that outlines the steps to take to mitigate the risk connected to ISO 27001 certification is termed as risk treatment plan. It is for this reason that the risk treatment strategy must be one that is tailored for your organization. Being a part of the certification procedure, the risk treatment plan is an essential component of the ISO 27001 system since it can obviously show the way to compliance and certification.

During the compliance process you will be required to write a risk treatment plan if at all you wish to be certified under ISO 27001.

Type of risks HNB finance might be face

- Cyber Security Risks:

  Phishing, social engineering, malware, ransomware attacks and Advanced Persistent Threats (APTs) are threats to financial institutions. These threats can lead to data encryption, data theft, system interruption, financial fraud and data breaches.

- Data Breach and Data Leakage Risks:

  Insider threats entail persons who are a part of an organization or have been contracted to offer their services in exposing or misusing and/or stealing information. Due to unsuccessful attempts of not securing data in the process of storage and transmission this may result in leakage of data and noncompliance with data protection laws such as GDPR.

- IT System and Application Risks:

  Software vulnerabilities and system downtime can lead to unauthorized access, malware injection, and disruptions in banking systems, causing critical financial losses and reputational losses.

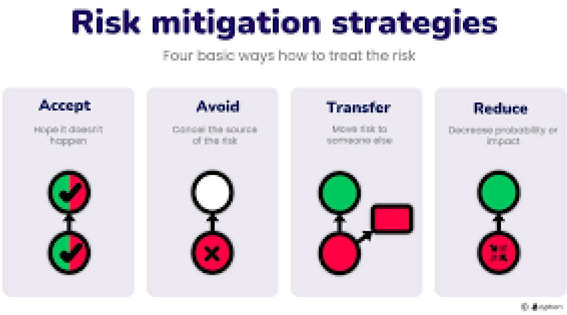
- Network and Infrastructure Risks:

  There are risks of DDoS attacks, resulting in service disruption and insecure network setting resulting in data loss for HNB Finance.

- Third-Party and Supply Chain Risks:

  Third party risks and supply chain risks are the next business risks that HNB Finance is exposed to because of the weaknesses of present in IT services and structures.

Risk Treatment Options


Risk mitigation strategies
Four basic ways how to treat the risk
Accept
Hope it doesn't happen
Avoid
Cancel the source of the risk
Transfer
Move risk to someone else
Reduce
Decrease probability or impact

- Mitigation: Applying security controls to a level at which the actual risk is made tolerable.
- Avoidance: The risk is removed by altering the business process or the activity that is creating the risk.
- Transfer: Transferring the risk with a third party as is the case with insurance or contracting out certain.
- Acceptance: Acknowledging the risk and choosing to accept it without additional controls if it falls within the risk appetite.

Risk Treatment Plan Development

The Risk Treatment Plan for HNB Finance is formulated based on identified risks, treatment options and ISO 27001:2022 controls, ensuring specific security controls, timelines and resources.

Security Controls Implemented

- Access Control & Cryptographic Controls
  - Multi-Factor Authentication (MFA)
  - Role-Based Access Control (RBAC)
  - Data Encryption
  - Human Resource Security & Communication Security
  - Phishing Simulations and Awareness Training
  - Email Filtering and Anti-Malware Solutions
- Information Security Aspects of Business Continuity Management
  - Disaster Recovery Plan (DRP)
  - Redundant Systems and Backup Solutions
- Asset Management & Compliance
  - Data Protection Impact Assessments (DPIAs)
  - Updated Data Handling Procedures
- Supplier Relationships
  - Third-Party Risk Management Processes
  - Contractual Clauses and Audits

Security Controls Implementation Plan

The purpose of this report is to offer a framework outlining the implementation of assumed security controls that responds to the identified risks and protect information assets meeting the ISO 27001:2022 standard relevant regulations and HNB Finances vision and mission.

Controls And Relevance to Risks

Control	Description	Relevance to Identified Risks	ISO 27001 : 2022 Controls
Multi-Factor Authentication (MFA)	Provide MFA to all employees and to all those people that have administrative access to the system to improve the access control security to the organization.	Reduces threats of invasion of privacy and stealing of identity, especially for systems involving customers' information and other financial transactions.	Access Control
Web Application Firewalls (WAFs)	Use WAFs in defending online banking applications and allied digital platforms against some of the inherent web app vulnerabilities including, SQL injection, cross site scripting (XSS) and DDoS.	Mitigates risks that may see web applications attacked therefore ensuring that the online banking services remain safe from such external threats as well as customers information.	Communication Security

Data Encryption	Use strong encryption standards (e.g., AES-256) to encrypt sensitive data both at rest and in transit to prevent unauthorized access and data breaches.	Reduces risks of data leaks by making sure that the data cannot easily be stolen even if intercepted or accessed by the wrong persons.	Cryptographic Controls
Endpoint Detection and Response (EDR)	Implement EDR solutions for real time investigations and occurrences that are suspicious in endpoints particularly workstations and/or servers.	Reduces the likelihood of a system getting infected by malware or any form of viruses or hacker intrusion apart from dealing with insider risks through enhanced threat identification and response to threats.	Operations Security
Disaster Recovery Plan (DRP)	Create and maintain the DRP with measures such as backup procedures and redundant alternatives that will allow the organization to carry on operation during a cyber-attack or other related disasters.	Reduces risks concerning business disruption and operating resilience by affirming that key business processes can be carried on or resumed in case of disruption.	Information Security Aspects of Business Continuity Management
Data Loss Prevention (DLP)	Use DLP solutions for the classification, tracking and control of sensitive data in the context of sending, receiving or transferring of data by email, cloud storage to other devices.	Reduces the risks of data leakage and loss due to the protection of data policies or restrictions concerning data transfer between networks or end user points.	Asset Management, Communication Security
Security Awareness and Training Programs	Employees should be trained and informed on security obligations and some of the security risks and precautions to be taken on a regular basis and when an incident is suspected.	Reduces risks that are associated with mistakes and ignorance by making it possible for every employee to comprehend his/her responsibilities in as a way of preserving information security besides knowledge on how to handle risks.	Human Resource Security

Resources Required for Implementation

Control	Resources Required	Responsible Parties
Multi-Factor Authentication (MFA)	Budget for MFA software and hardware tokens, IT personnel for deployment and configuration, training resources for users.	IT Security Team, Information Security Manager
Web Application Firewalls (WAFs)	WAF appliances or cloud-based WAF services, IT Security Engineers, budget for procurement and maintenance.	IT Security Team, Digital Banking Team
Data Encryption	Encryption tools and software, encryption key management solutions, IT and security personnel for configuration.	IT Team, Information Security Manager
Endpoint Detection and Response (EDR)	EDR solutions (software and licenses), cybersecurity analysts, SIEM integration tools.	IT Security Team, Incident Response Team
Data Loss Prevention (DLP)	DLP solutions (software and licenses), IT security team for configuration and monitoring, budget for training and awareness.	IT Security Team, Data Protection Officer
Disaster Recovery Plan (DRP)	Backup solutions, disaster recovery sites (primary and secondary), crisis management team, tools for testing and drills.	Business Continuity Manager, IT Team
Security Awareness and Training Programs	E-learning platforms, content developers, cybersecurity experts, HR involvement for coordination.	Security Awareness Coordinator, HR Team
Third-Party Risk Management (TPRM)	Vendor risk assessment tools, legal and compliance teams, budget for audits and assessments.	Vendor Management Team, Compliance Officer

Examples for Some Controls Implementation Steps

- Multi-Factor Authentication (MFA)

  Implementation Steps:

  - Phase 1: Carry out a requirements analysis to identify a more suitable MFA solution such as OTP through SMS mobile application-based authentication or physical tokens.
  - Phase 2: Use MFA on all privileged accounts and to all high-risk systems (e. g. Core banking, financial reporting systems).
  - Phase 3: Implement MFA in all organizational levels and the vital areas of risk exposure that include email, remote access VPNs and cloud applications.

- Web Application Firewalls (WAFs)

  Implementation Steps:

  - Phase 1: Assess current web applications and identify vulnerabilities and attack vectors.
  - Phase 2: Place WAFs in front of key applications, adjust configuration rules to compliance with the company's security standards.
  - Phase 3: Perform simulation to prove the credibility of WAFs in counteracting the attacks.

- Data Encryption

  Implementation Steps:

  - Phase 1: Use encryption for databases, stored files and backup data.
  - Phase 2: Encryption in transit can be employed by using the SSL/TLS standards in internal and external communications.
  - Phase 3: It is also advisable to conduct a survey every now and then to check whether encryption is well implemented or not.

Monitoring & Reporting

- Progress Tracking:

  A centralized project management tool like Microsoft Project or Jira will be utilized to monitor the implementation of each control, providing stakeholders with visibility and task assignments**.**

- Weekly and Monthly Reports:

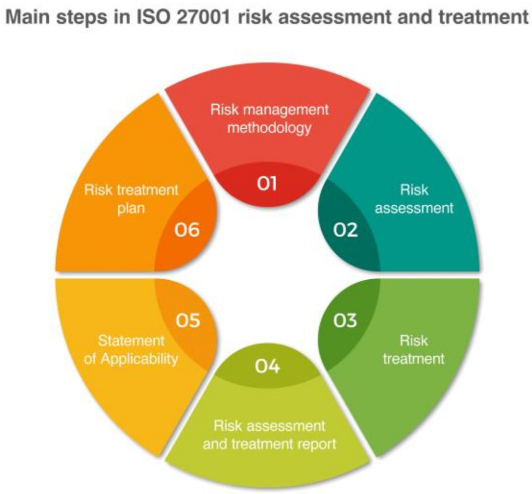
  The project team will prepare weekly progress reports for the Information Security Manager, while monthly summary reports will be presented to the Board Integrated Risk Management Committee.

- Key Performance Indicators (KPIs):

  Metrics for all the controls as highlighted above will include things like time to deploy the control, rate of completion for the phishing simulation and response times to the DRP drills among other factors.

- Internal Audits:

  The Internal Audit team will conduct regular audits to assess the effectiveness of controls, identify gaps and suggest improvements with findings shared with the Board Audit Committee for review.


Main steps in ISO 27001 risk assessment and treatment
Risk management methodology
01
Risk assessment
02
03
Risk treatment
04
Risk assessment and treatment report
05
Statement of Applicability
06
Risk treatment plan

Security Awareness & Training Plan

As for the human factor, HNB Finance is now launching a security-awareness program to cover all the employees and train them in information security policies, procedures, and measures to avoid personnel mistakes and generate security-awareness among all the company's staff.

Training Program

The Security Awareness and Training Program will be structured around three core components:

1. General Awareness Training for all employees.
2. Role-Specific Training for specialized roles such as IT staff, developers, and data handlers.
3. Management and Executive Training for senior leadership and decision-makers.

Training Materials & Strategies

- General Employee:
  - Target Audience:
    All staff members, including customer service representatives, administrative staff and operational personnel
  - Training Materials: E-Learning Modules: Self-paced online courses covering fundamental topics such as:
    - Introduction to Information Security.
    - Password Management and Multi-Factor Authentication (MFA).
    - Phishing Awareness and Social Engineering.
    - Safe Internet and Email Practices.
    - Data Handling and Protection.

- Training Strategies:
    - Simulated Phishing Exercises: Phishing should be conducted often with the aim of identifying how keen the employees are in reporting phishing scams.
    - Quizzes and Assessments: Add a brief quiz at the end of every module in order to check the knowledge of the material.
    - Gamification: Employ application of game-like features like top performers' list and incentives that will motivate the learners to join the training courses and complete the modules.

- IT Staff and Security Professionals
    - Target Audience:

      IT personnel, system administrators, network engineers, and cybersecurity professionals
    - Training Materials:
        - Advanced E-Learning Modules: Courses on topics
        - Hands-On Workshops: Instructor-led sessions
        - Guides and Playbooks: Detailed playbooks for incident response, threat intelligence, and security monitoring
    - Training Strategies:
        - Capture-the-Flag (CTF) Exercises: Schedule CTF challenges to enhance the problem solving and the general practical experiences in a competition like manner.
        - Red-Blue Team Exercises: The red-blue team exercise is the best to be used to practice attack and defense since both require practice.

    - Threat Intelligence Sharing: Daily or weekly updates on new cyber threats, methods used by the attackers and existing security bulletins regarding the operation of the financial sector.

- Management and Executives
  - Target Audience:

    Senior management, board members, and decision-makers.
  - Training Materials:
    - Executive Briefing Sessions: Specific meetings dealing with the essential topic of cybersecurity and risk management as well as compliances.

      Case Studies and Scenarios: Real-life cases of cyber incidents that occurred in the financial industry and their implications on business.
    - Regulatory and Compliance Workshops: Awareness and sensibilities on specific rules applicable for carrying ON business and corporate operations and management (e.g., GDPR, Central Bank directives).
  - Training Strategies:
    - Tabletop Exercises: Organize daily and revolving high Frequency apart Time tabletop exercises that concern high impact cyber incidents to test decision making, communication methods and response.
    - Risk Management Workshops: Workshops focused on aligning cybersecurity strategies with organizational risk appetite and business objectives.
    - Key Metrics and Dashboards: Make information available in the form of performance reports on security performance in terms of results achieved with benchmarks and possible threats revealed for executive management.

Delivery Methods

- E-Learning Platforms:
  Available to the learner at any time and at any place, thus, the fact that the employee can do the training at one's own convenience.

- In-Person and Virtual Workshops:
  Instructor-led sessions for hands-on experience and interactive learning.

- Simulations and Drills:
  Realistic simulations (phishing drills, disaster recovery exercises) to reinforce learning through practice.

- Regular Updates:
  Weekly bulletins online seminars and e-mail alerts to ensure the employees of the company are up to date with the latest risks and measures taken.

Metrics for Measuring Effectiveness

- Training completion rates:
  Measure the percentage of employees who complete the assigned training modules within the specified period.

- Assessment scores and knowledge retention:
  Track scores from quizzes and assessments conducted after each training module to evaluate knowledge retention and understanding.

- Incident response times and effectiveness:
  Measure the time taken to detect, respond to, and recover from simulated incidents during red-blue team exercises and tabletop exercises.

Continuous Improvement Plan

- Regular Review and Updates:

  The training material developed will be periodically revised every at least three months to meet the new threats, risks and changes in provisions.

- Feedback Loop:

  Through surveys, focus groups and debriefing sessions with employees and management suggestions and comments for organizational development will be obtained.

- Performance Analysis:

  A post program yearly assessment will involve an evaluation of the program’s effectiveness yearly based on the laid down metrics and KPIs.

Incident Response Plan (IRP)

A Cybersecurity Incident Response Plan is essentially a text-based document aimed at assisting cybersecurity and information technology gurus on how best to approach major security threats including ransomware, data leaks, breaches or loss of sensitive data. Most effective incident response plans consist of four phases according to the National Institute of Standards and Technology (NIST) These are preparation, detection and analysis, containment, eradication and recovery and post event activities.

People
Incident
Response
Plan
Technology
Process

Why Need an Incident Response Plan?

It can also be said that businesses must have CSIRP as it is obligatory now after the acts were passed and is considered a sound strategy in the modern world. If plans are not properly developed, then both management and security teams may wind up wasting more money than they should on mistakes and could respond to cyber-attacks that happen later than they should, which gives cyber attackers more time to cause more damages. Employees and business partners who might doubt the management team's expertise may become enraged about this. Specific CSIRPs also assist in establishing organizations' requirements on reporting the breach to the authorities and revealing information in 72 hours under the GDPR. The authorities can penalize a company for not meeting the requirements of these standards through fines.

Incident Response Team (IRT)

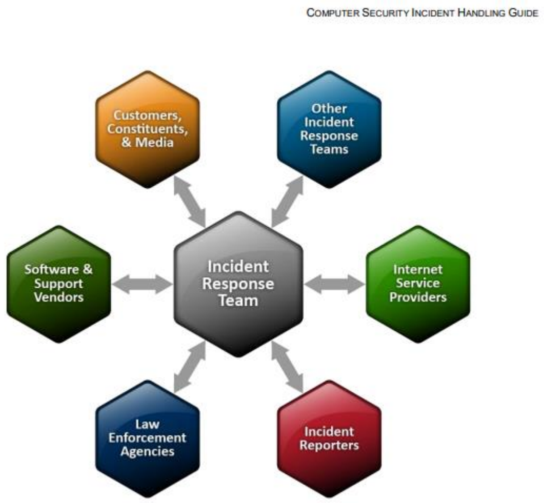

COMPUTER SECURITY INCIDENT HANDLING GUIDE
Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Figure 2-1. Communications with Outside Parties

- Incident Manager (IM)
  - Role: The Incident Manager again leads the whole process of managing incidents right from the identification of an incident to solving of that incident. In an event he takes the overall discretion of what has occurred and the resultant investigation.
  - Responsibilities:
    - Coordinate all incident response activities and resources.
    - Communicate with senior management, legal department, compliance and any other third parties.
    - Ensure accurate documentation of the incident and response actions.
- Communication Lead (CL)
  - Role: The Communication Lead manages internal and external communication related to the incident.
  - Responsibilities:
    - Draft internal and external communication statements.
    - Coordinate with the public relations department, customer support and other states agencies with regards to information sharing.
    - Manage communication channels to prevent misinformation.

- IT Support Team (ITST)
  - Role: The IT Support Team is responsible for technical analysis, containment, and recovery of affected systems.
  - Responsibilities:
    - Identify affected systems and determine the scope and impact of the incident.
    - Carry out containment, elimination as well as recovery steps.
    - Provide technical support in restoration and recovery of damaged systems and sustaining adequate testing processes.
- Cybersecurity Analyst (CSA)
  - Role: The Cybersecurity Analyst’s functionality is to analyze the problem in detail to ascertain its sources and gather intelligence for the response actions.
  - Responsibilities:
    - Use system logs, network traffic and other similar information to determine the kind of attack that was launched.
    - Select identify of compromises (IOCs) and map them to comprehend tactics employed by the attacker.
    - Provide threat intelligence updates to the Incident Manager and IT Support Team.
- Legal and Compliance Officer (LCO)
  - Role: Responsible for making sure that all of the activities related to handling incidents are done in accordance with the laws, rules and regulations as well as agreements.
  - Responsibilities:
    - Brief the IRT on legal and compliance issues as it pertains to the incident or occurrence.
    - Ensure all regulatory and law enforcement contacts in regard to data breaches or any other compliance issues and customers are handled.
    - Make sure that all the facts are collected and kept in such a way, which would be allowed in the court.

Incident Classification & Prioritization

HNB Finance will categorize events and degree of risk in relation to the overall operations, resources and Company reputation and compliance with laws and regulations.

Classification	Description	Impact	Examples
Minor	Incidents with minimal impact on systems, operations, or data. Can be managed and resolved quickly by the IT team.	Low	Incidents that significantly impact critical systems, data, or business operations, requiring cross-functional response.
Moderate	Incidents that have a noticeable impact on specific systems or processes, potentially disrupting services.	Medium	Successful phishing attacks on a few employees, malware infection in a non-critical system.
Major	Incidents that significantly impact critical systems, data, or business operations, requiring cross-functional response.	High	Ransomware attack affecting core banking systems, data breach involving customer information.

Incident Response Procedures

- Detection and Identification
  - Monitor: Real-time analysis of traffic syslog messages and endpoints with help of SIEM, IDS/IPS, EDR and UEBA.
  - Alerting: Automatically generate alerts for potential security incidents based on predefined rules and thresholds.
  - Verification: The IT Support Team or Cybersecurity Analyst verifies the alerts to confirm the incident, determining its nature and scope.

- Analysis
  - Initial Assessment: Assess the incident's impact and severity based on the incident classification criteria.
  - Evidence Collection: Collect logs, network traffic, and other relevant data for further analysis while preserving the chain of custody for potential legal investigations.
  - Root Cause Analysis: Cybersecurity Analysts perform root cause analysis to identify the attack vector, affected assets, and potential vulnerabilities.
- Containment
  - Short-Term Containment: Isolate affected systems from the network to prevent further spread. This may include disconnecting the machines, banning certain IPs or even restricting users in some way.
  - Long-Term Containment: Use temporary fixes if possible while also referencing regain control of the systems if possible while at the same time tightening security measures in the area.
- Eradication
  - Remove Threats: Elimination of all forms of viruses, hackers unintended means or ‘back doors’ that the attackers create.
  - Validate System Integrity: Make sure that all the implicated systems are free from problems such as malware, vulnerabilities and other poor configurations.
- Recovery
  - System Restoration: Restore systems and services from backups or clean images, ensuring they are fully functional and secure.
  - Monitoring for Recurrence: Monitor restored systems for signs of recurrence and apply additional controls if necessary.
- Communication
  - Internal Communication: Regularly update senior management, IT teams, and affected departments on the incident status and activities under way.
  - External Communication: Inform customers, regulators, and law enforcement as required, ensuring compliance with regulatory obligations and maintaining transparency.

Post-Incident Review

The main points of conducting a Post-Incident Review (PIR) include the ability to refine the procedure involved for the processes of responding and preventing future incidents.

- Review Meeting:

  Conduct a review meeting involving all IRT members and relevant stakeholders within two weeks of incident resolution.

- Documentation:

  Document all aspects of the incident, including detection, response actions, containment measures, eradication steps, recovery, and communication efforts.

- Root Cause and Impact Analysis:

  Evaluate whether the incident can be considered root cause analysis of the effects on the business, data and customer's trust.

- Identify Gaps and Areas for Improvement:

  Determine prior practices for handling and responding to an incident and see what weaknesses may have existed prior to the incident that contributed to its occurrence or to the time needed to manage the situation.

- Develop Recommendations:

  Formulate recommendations for improving incident response capabilities, including updating policies, implementing new controls, and enhancing training programs.

- Action Plan:

  It is vital to come up with an action plan on how to execute the recommendations, the individuals charged with the responsibility of implementing the recommendations and the time required to finish the task at hand.

- Reporting:

  Prepare the findings and the action plan in a report and make a presentation to the BIRMC followed by presenting the same findings and action to the BAC for approval.

Continuous Improvement and Readiness

- Regular Testing and Exercises
- Ongoing Training
- Annual Review and Update
- Integration with the ISMS

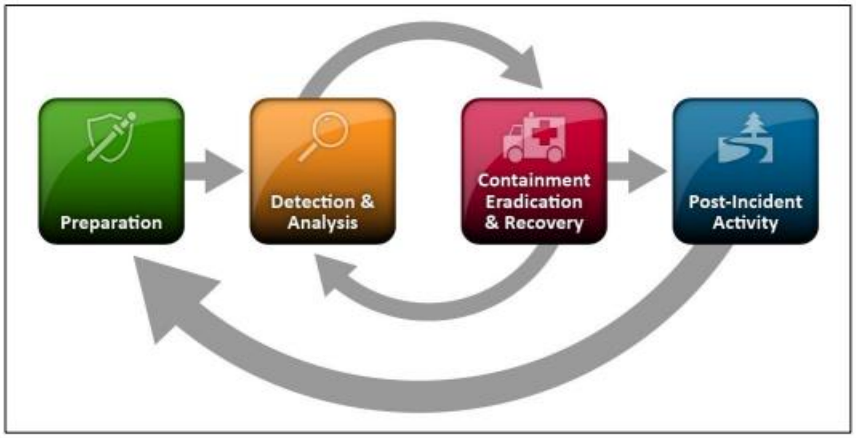
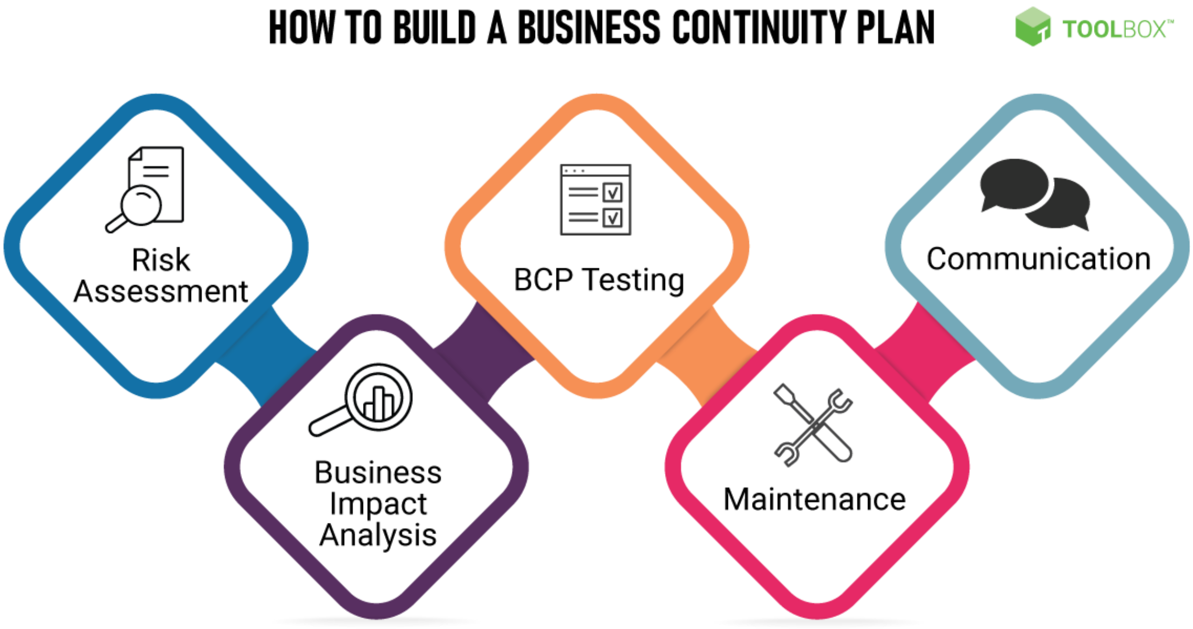


Figure 3-1. Incident Response Life Cycle

Business Continuity Plan (BCP)

A business continuity plan is an official document which contains a list of organization's activities reveals the list of significant systems and processes and describes how these processes are to be continued in case of an unforeseen incident. It deals with threats such as hackers, diseases outbreaks, floods, fire and employees' mistakes and is crucial for the sustainability and image of a firm. Effective BCP reduces the chances of costly power outages or IT outages occurring and hence should be well developed. IT administrators typically draft the plan, and executive staff provides expertise and oversight to ensure the BCP is updated on a regular basis.



Business continuity planning steps

The business continuity planning lifecycle contains these five steps:

- Step 1: Analysis
  - Conduct an "as-is" analysis to identify critical activities that must continue during a disruption.
  - Engage stakeholders to agree on what activities need peak performance, which can be paused, and which can operate at a reduced level.
  - Prioritize activities for continuous delivery versus recovery and estimate the time required for recovery.
  - Consider the financial impact of downtime and client-friendly policies, which can lead to lost revenue and increased costs.
- Step 2: Risk Assessment
  - Evaluate internal and external threats to critical business activities, considering all potential scenarios.
  - Familiarize with the existing risks related to a particular area such as natural disasters such as hurricanes, earthquakes, epidemics, fire, floods etc.
  - Assess management and client tolerance for reduced capacity operations.
  - Identify vulnerabilities and develop strategies to avoid, reduce, or mitigate risks.
- Step 3: Develop Recovery Procedures
  - Outline detailed, step-by-step procedures to respond to incidents, focusing on protecting people, operations, and assets.
  - Consider changing the operating model to be more resilient (e.g., remote work, multiple sites, hybrid workforce).
  - Integrate automation and technology to improve scalability, productivity, and resilience.
  - Organize recovery teams, define recovery tasks, and develop technology and worksite recovery plans.
  - Address personnel impacts, including safety, communication, and post-incident support.
- Step 4: Communicate & Integrate
  - Ensure the plan is known, accessible, and integrated into the company's culture and policies.
  - Use simple terminology to make the plan easy to understand in stressful situations.

  - Make the plan available in hard copy and electronic formats and consider using a web portal for easy access.
  - Prepare pre-drafted messages for quick communication with key stakeholders (community, customers, suppliers).
- Step 5: Test, Train & Maintain
  - Regularly test the plan to ensure it works and that staff know what to do and how to collaborate.
  - Conduct different types of exercises (seminar, table-top, live) to train staff and familiarize them with the plan.
  - Continuously update the plan based on test results and changes in the business environment to ensure its effectiveness.

Threats To Face

Natural Disasters
Man-made Disasters
Utility Failures
Cybersecurity Attacks
Intentional Sabotage

- Global Pandemics
  - Impact: Forces employees to work from home, increases demand for certain items, and disrupts supply chains.
  - Mitigation Strategies:
    - Develop a strongest disaster communication plan.
    - Envision offsite collaboration and necessary business operations.
    - Identify alternative suppliers and products to avoid single points of failure.
    - Use current experiences to improve future response plans.

- Power Outages
  - Impact: Loss of communication lines, power, and water can disrupt operations, damage physical assets, and cause productivity loss.
  - Mitigation Strategies:
    - Prepare for unexpected utility outages.
    - Consider backup power solutions and strategies to minimize downtime.
- Natural Disasters
  - Impact: Encompasses meteorological disasters such as hurricanes, tornadoes, tsunamis and other geological disasters including earthquakes, volcanic eruptions, wildfires. These can lead to substantial loss of immovable properties and major interferences with supply systems.
  - Mitigation Strategies:
    - Disaster recovery planning should be used to guard the organization’s physical and electronic properties.
    - Diversification of supply should be encouraged as well as preparing for supply disruptions.
- Cybersecurity Threats
  - Impact: These attacks include data theft, ransomware attacks, SQL injection and DDoS that threatens business data and IT networks.
  - Mitigation Strategies:
    - Implement robust cybersecurity measures, including data backup and recovery plans.
    - Follow a cybersecurity checklist to identify potential vulnerabilities and develop preventative measures.

Benefits Of Business Continuity Plan

- Minimize Downtime and Losses
  - A BCP ensures that businesses can quickly implement necessary actions to keep operations running during disruptions, minimizing downtime and financial losses.
  - It includes contingencies such as supporting remote work if physical offices are inaccessible or having backup servers for power outages, ensuring continuous operations and revenue flow.
- Anticipate Risks and Threats
  - Periodic reviews and conversations about the BCP help to discover possible threats such as war, hurricane, viral outbreak, hack or anyhow data leak.
  - By understanding these risks, businesses can prevent losses by developing specific response and recovery procedures.
- Ensure Customer Confidence and Safeguard Reputation
  - Efficient handling of crisis situations and rapid restoration increases customers' confidence, which shows stability and failure is not an option.
  - A BCP also increases customer trust in the company as regards protection of their data and the assurance of service levels, thus fostering the retention of those clients and steadily creating a good reputation in the market.
- Enhance Employee Safety and Well-being
  - A BCP prioritizes employee safety, covering both physical and mental well-being, especially during crises.
  - Clear communication and support structures, such as remote work arrangements and mental health programs, foster employee confidence, productivity, and vigilance against security threats.
- Gain Competitive Advantage
  - When a business organization has a good BCP it can regain normalcy soon after a disruption and continue providing service which will enhance its image as a dependable and stable brand.
  - This preparedness makes them ready for any interruption than rivals who can even take time to recover from interruption thus improving corporate governance as well as customer relations.

Faced Challenges & Learned Lessons

Challenges Faced

- Resource Allocation and Budget Constraints:

  Implementing ISO 27001 requires considerable assets, together with human, monetary, and technological. For HNB Finance, aligning the assignment with their cutting-edge finances might also additionally had been a venture, specifically if the employer grows to be not definitely prepared for the remarkable requirements of certification.

- Complexity of Risk Assessment:

  Conducting an intensive hazard assessment in a financial organization may be hard due to the extent and sensitivity of economic facts. Identifying, evaluating, and prioritizing risks required an in-intensity knowledge of each economic operations and protection threats.

- Employee Resistance to Change:

  Introducing new security features and guidelines can cause resistance from employees who can also view them as disruptive. Ensuring that ever one employee, especially humans with little previous know-how of facts safety, understood the significance of the ISMS may additionally have required big effort.

- Integration with Existing Systems:

  HNB Finance likely faced problems integrating ISO 27001 requirements with its pre-present IT systems and safety protocols. Ensuring clean implementation without disrupting commercial enterprise continuity is frequently complicated in economic institutions.

- Maintaining Compliance Amid Changing Regulations:

  Financial corporations feature beneath stringent felony and regulatory frameworks. Staying compliant with every ISO 27001 and industry-unique policies (like Central Bank of Sri Lanka directives) may be a big assignment, requiring non-stop tracking and model.

Learned Lessons

- Cross-Departmental Collaboration is Key:

  Successful ISMS implementation required coordination all through departments (IT, finance, HR, and many others.). Effective collaboration ensured that regulations had been tailor-made to fulfill the specific goals of every department.

- Importance of Employee Training:

  The safety interest and training packages were essential in gaining worker purchase-in and ensuring that everyone understood their function in retaining the ISMS. Continuous schooling and regular updates on the device's blessings helped overcome preliminary resistance.

- A Comprehensive Risk Management Approach:

  The threat assessment highlighted the need for a proactive, ongoing threat management method. Developing a complete hazard sign up and treatment plan allowed HNB Finance to cope with capability vulnerabilities in a set up way.

- Documentation and Regular Audits:

  Documenting every step of the implementation approach and task everyday audits helped hold the mission on target. It also led to the eventual ISO 27001 certification with a useful resource for proof of compliance and due diligence.

- Business Continuity Plan (BCP):

  The implementation of ISO 27001 has given us a sharper understanding of the importance of continuity for commercial enterprise employers, especially in financial management The improvement of a robust BCP ensured that HNB Finance needs to maintain operations inside the face of protection incidents or disruptions.

Summary

The assignment on ISO 27001:2022 implementation for HNB Finance specializes in setting up an Information Security Management System (ISMS) compliant with worldwide standards. The document information the scope of the ISMS, overlaying important departments and capabilities like IT, operations, and customer service, whilst aside from non-vital regions along with marketing. It outlines roles for team participants, such as undertaking control, threat assessment, policy improvement, and compliance monitoring. The report emphasizes the significance of risk management, security recognition, and education for group of workers. HNB Finance's commercial enterprise capabilities, along with digital banking and microfinance, are supported by the ISMS to mitigate dangers including cyberattacks and statistics breaches. Key deliverables encompass a hazard evaluation file, a danger remedy plan, and security controls like encryption, multi-issue authentication, and net application firewalls. The venture also highlights demanding situations like useful resource allocation and employee resistance, while emphasizing the importance of documentation, pass-departmental collaboration, and continuous improvement in securing economic records.

References

https://www.iso.org/standard/27001

https://www.itgovernance.eu/blog/en/a-9-step-guide-to-implementing-iso-27001

https://www.itgovernanceusa.com/blog/iso-27001-registrationcertification-in-ten-easy-steps

https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-isms/

https://chazeypartners.com/article/5-steps-to-develop-a-robust-business-continuity-plan/

https://www.azeusconvene.com/articles/why-your-business-needs-a-business-continuity-plan

https://www.hnbfinance.lk/

https://www.hnb.net/images/annual_reports/2023/integrated-report-2023.pdf

https://cdn.cse.lk/cmt/upload_report_file/373_1678180085123.pdf

https://www.hnb.net/images/annual_reports/2021/corporate-governance-risk-management-report-2021.pdf

https://www.hnbfinance.lk/wp-content/uploads/2019/08/HNB-Finance-Limited-AR-2018-19-2.pdf

https://www.iso.org/standard/iso-iec-27000-family