Sri Lanka Institute of Information Technology

Assignment Report 02

IE3102

A picture containing text, clipart

Description automatically generated

**2. Business Process Implementation Plan**

**Enterprise Standards for Information Security – IE3102**

**B.Sc. (Hons) in Information Technology**

**Student Details**

|  |  |
| --- | --- |
| **Student ID** | **Student Name** |
| IT22560094 | Ranasinghe R.A.D.T.M |

**Table of Contents**

[**Introduction** 4](#_Toc179797416)

[**Business Process Implementation Plan** 5](#_Toc179797417)

[**Stage 1: Assemble a team and develop a plan [1].** 5](#_Toc179797418)

[**Stage 2: Scope and baseline ISMS [2] [1]** 7](#_Toc179797419)

[**Stage 3: ISMS Implementation [1] [2].** 8](#_Toc179797420)

[**Stage 4: Define and implement the risk management process [3] [1].** 9](#_Toc179797421)

[**Stage 5: Measure, Monitor, review, and certify ISMS [1] [3].** 11](#_Toc179797422)

[**References** 13](#_Toc179797423)

# **Introduction**

This Business Process Implementation Plan provides a detailed roadmap for organizations aiming to successfully implement the chosen IT standard. The plan is designed to guide organizations through the process, step by step, ensuring clarity on timelines, assigned responsibilities, and resource allocation. Each stage outlined in this plan is meticulously crafted to streamline the integration of the standard into the organization's framework, ultimately leading to compliance and certification. This comprehensive approach not only reinforces information security but also strengthens the organization's overall operational capacity.

# **Business Process Implementation Plan**

## **Stage 1: Assemble a team and develop a plan [1].**

1. Select a Competent Project Manager

The starting point for implementing the Information Security Management System (ISMS) is the selection of a capable project manager. This individual should have expertise in information security and be capable of leading a team and providing guidance to managers.

1. Assemble the Implementation Team

A team of employees will be required to support the project manager. Senior management may choose team members personally or delegate this authority to the team leader.

1. Develop a Project Mandate

The newly formed team should collaborate to create a project mandate, which answers essential questions:

* What are our objectives?
* When will we complete the project?
* What is the estimated cost?
* Is there management support for the project?

1. Initiate Implementation Planning

The project mandate will serve as a foundation for the implementation team to start developing a comprehensive plan and risk register for their information security goals.

1. Establish High-Level Policies for ISMS

During this stage, the team should lay down high-level policies for the ISMS, addressing key aspects such as:

* Roles and responsibilities.
* Guidelines for continuous improvement.
* Strategies for internal and external communication about the initiative.

1. Adopt the Plan-Do-Check-Act Approach

Choose the Plan-Do-Check-Act (PDCA) methodology as the constant improvement approach. This method involves continuous cycles of planning, executing, monitoring, and adapting to improve the ISMS.

1. Develop an ISMS Policy

As part of the planning process, create a comprehensive Information Security Management System (ISMS) policy. This policy will define the overarching principles and objectives of the ISMS.

## **Stage 2: Scope and baseline ISMS [2] [1]**

1. Understand ISO 27001 Requirements

Begin by understanding the ISO 27001 requirements as outlined in Clauses 4 and 5 of the standards. This provides the foundation for defining the scope of your Information Security Management System (ISMS).

1. Acknowledge Organizational Relevance

To ensure that the ISMS aligns with your organization's needs, acknowledge all aspects that are relevant to your business. Consider both internal and external factors that impact your organization.

1. Define the Scope of Your ISMS

The deployment of your ISMS and the selection of information storage locations depend on the scope of your ISMS [1]. Determine the right scope that suits your organization. Discuss the considerations associated with broad and narrow scopes, highlighting their impact on management and security.

1. Identify Security Baseline

Define the security baseline, which represents the minimum level of security activities necessary for your organization to conduct business securely [1]. ISO 27001's risk assessment helps identify critical security weaknesses and the ISO 27001 procedures needed to mitigate these risks [1].

1. Consider the Context of the Organization

Explore the context of the organization as described in ISO 27001 [5]:

* Understand the organization and its context - Identify external and internal factors affecting the organization's purpose and its ability to achieve its information security management system goals.
* Understand the needs and expectations of interested parties - Determine relevant interested parties, their requirements, and how these will be addressed through the ISMS.
* Determine the scope of the information security management system - Define the boundaries, applicability, and interfaces related to the ISMS, taking into account external and internal factors, requirements, and dependencies.
* Establish the information security management system - Define and document the ISMS, including processes and interactions, by ISO 27001 requirements.

## **Stage 3: ISMS Implementation [1] [2].**

1. Organize an Information Security Steering Committee

Begin by forming an information security steering committee, which will play a key role in overseeing the ISMS implementation.

1. Document Information Security Policy and Other Policies

Develop and document the information security policy, along with other related policies that define the organization's stance on specific issues, such as acceptable use and password management.

1. Methodology for Implementing ISMS

Adopt a methodology for implementing the ISMS. The ISO 27001 standard emphasizes a "process approach" to continual improvement for managing information security. While it doesn't specify a particular methodology, organizations have the flexibility to choose their preferred method or continue with an existing model.

1. Four-Tier Strategy for Document Structure

Implement a four-tier strategy for your document structure:

* Start with top-level policies that define the organization's position on specific issues.
* Develop procedures to enact the requirements of these policies.
* Create work instructions that detail how employees should meet the policies and procedures.
* Maintain records that track the implementation of procedures and work instructions.

1. Understanding the ISMS Framework

Gain a comprehensive understanding of the ISMS framework, as outlined in clauses 4 and 5 of the ISO 27001 standard.

Focus on defining the scope of your ISMS, and determining which parts of your organization will be protected. Establishing an appropriate scope is a crucial aspect of your ISMS implementation project. If the scope is too narrow, it may leave critical information exposed, jeopardizing the organization's security. If the scope is overly broad, the ISMS may become too complex to effectively manage.

## **Stage 4: Define and implement the risk management process [3] [1].**

1. Risk Management as the Heart of ISMS

Understand that risk management is the core element of an ISMS. It involves identifying and managing organizational risks.

1. Identification of the Organization's Risk Management Process

Emphasize the importance of identifying the organization's risk management process, which is essential for managing information security risks effectively.

1. Risk Assessment Framework

Detail the five essential steps of risk assessment:

* Establish a risk assessment framework.
* Identify risks.
* Analyze risks.
* Evaluate risks.
* Select risk management options.

1. Risk Treatment Strategies

Explain the four possible strategies for addressing risks:

* Accepting the risk.
* Applying controls to mitigate the risk.
* Avoiding the risk completely.
* Transferring the risk to another party.

Highlight that building security controls, ensuring staff competency, and creating a competence review process are key components of implementing a risk treatment plan.

1. Baseline Security Controls

Define an organization's security baseline as the minimum level of activity required to conduct business securely.

Stress that this baseline should be established based on the information collected during the ISO 27001 risk assessment.

1. Risk Assessment Process

Describe the importance of the risk assessment process.

Explain that the process involves identifying, evaluating, and assigning values to threats to determine the most significant risks.

Clarify that the next step is deciding how to handle these risks, which can include treating them with information security controls, avoiding them, sharing the risk through insurance or agreements, or accepting the risk if it is not significant.

Mention that any risks that are treated should be documented in a Statement of Applicability (SoA), which should explain the selection and omission of ISO 27001 controls and the reasoning behind these choices.

## **Stage 5: Measure, Monitor, review, and certify ISMS [1] [3].**

1. Performance Evaluation (Monitoring, Measurement, Analysis, and Evaluation)

* Determine what aspects of the ISMS need to be monitored and measured, including information security processes and controls.
* Define the methods for monitoring, measurement, analysis, and evaluation to ensure valid results.
* Specify when monitoring and measuring activities will occur and who will be responsible.
* Identify when and by whom the results from monitoring and measurement will be analyzed and evaluated.
* Ensure that documented information is available as evidence of the results.
* Evaluate the performance of the information security management system and its effectiveness.

1. Internal Audit

* Conduct regular internal audits at planned intervals to assess the conformance of the ISMS to organizational requirements and the ISO 27001 standard.
* Establish an internal audit program with defined criteria, scope, and responsibilities.
* Select auditors and conduct audits to ensure objectivity and impartiality.
* Report the results of audits to relevant management.
* Maintain documented information as evidence of the audit program and results.

1. Management Review

* Top management should review the organization's ISMS at planned intervals to ensure its suitability, adequacy, and effectiveness.
* Consider inputs for the management review, including the status of actions from previous reviews, changes in external and internal issues, feedback on information security performance, and opportunities for continual improvement.
* Review and make decisions related to continual improvement opportunities and changes to the ISMS.
* Document the results of management reviews.

1. Continual Improvement

* Commit to continually improving the suitability, adequacy, and effectiveness of the ISMS.

1. Nonconformity and Corrective Action

* Address nonconformities by taking corrective actions that control and correct the nonconformity and deal with its consequences.
* Evaluate the need for actions to eliminate the causes of nonconformity, review the nonconformity, and determine its causes.
* Implement necessary corrective actions.
* Review the effectiveness of corrective actions and make changes to the ISMS if required.
* Document information on the nature of nonconformities and any subsequent actions taken, as well as the results of corrective actions.

1. Certification Audit Preparation

* If pursuing ISO 27001 certification, prepare for an external audit.
* Understand that the certification audit involves an initial audit to assess ISMS compliance with ISO 27001 specifications. A more in-depth investigation may follow if the auditor is satisfied.
* Carefully select a certification body that is accredited by a national certification body to ensure a review is genuinely in compliance with ISO 27001.

# **References**

|  |  |
| --- | --- |
| [1] | "iso-27001-checklist-a-step-by-step-guide-to-implementation,"[Online].Available:  https://www.itgovernance.co.uk/blog/iso-27001-checklist-a-step-by-step-guide-to-implementation |
| [2] | "Information-security-Edition-2022-Risk-management-Management-systems-The-ISO-IEC-27001-2022-standard-The-ISO-IEC-27002-2022-controls,"[Online].Available:  https://www.scribd.com/read/554170151/Information-security-Edition-2022-Risk-management-Management-systems-The-ISO-IEC-27001-2022-standard-The-ISO-IEC-27002-2022-controls#. |
| [3] | ISO/IEC, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," *Third edition 2022-10,* 2022. |