Sri Lanka Institute of Information Technology

A picture containing text, clipart

Description automatically generated

Assignment Report 02

IE3102

**4. ISO 27001(ISMS) Implementation for an Organization**

**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 5**](#_Toc179803096)

[**Implementing the ISO 27001:2022 standard 6**](#_Toc179803097)

[**1. Scope 6**](#_Toc179803098)

[**2. Normative references 6**](#_Toc179803099)

[**3. Terms and definitions 6**](#_Toc179803100)

[**4. The context of the organization and the scope of the ISMS 6**](#_Toc179803101)

[**4.1 The context of the organization 7**](#_Toc179803102)

[**4.2 The scope of the ISMS 7**](#_Toc179803103)

[**4.3 Information security management system 8**](#_Toc179803104)

[**5. Leadership 9**](#_Toc179803105)

[**5.1 Information security policy 9**](#_Toc179803106)

[**5.2 Roles and responsibilities 10**](#_Toc179803107)

[**6. Planning 11**](#_Toc179803108)

[**6.1 Actions to address risks and opportunities 11**](#_Toc179803109)

[**6.1.1 Information security risk assessment 12**](#_Toc179803110)

[**6.1.1.1 Establishing Risk Criteria 12**](#_Toc179803111)

[**6.1.1.1 Ensuring Consistency 12**](#_Toc179803112)

[**6.1.1.2 Identifying Risks 12**](#_Toc179803113)

[**6.1.1.3 Analyzing Risks 12**](#_Toc179803114)

[**6.1.1.4 Evaluating Risks 13**](#_Toc179803115)

[**6.1.2 Information security risk treatment 13**](#_Toc179803116)

[**6.1.2.1 Selecting Treatment Options 13**](#_Toc179803117)

[**6.1.2.2 Determining Necessary Controls 13**](#_Toc179803118)

[**6.1.2.3 Control Comparison 13**](#_Toc179803119)

[**6.1.2.4 Statement of Applicability 13**](#_Toc179803120)

[**6.1.2.5 Risk Treatment Plan Formulation 14**](#_Toc179803121)

[**6.1.2.6 Approval and Acceptance 14**](#_Toc179803122)

[**6.2 Information security objectives and planning to achieve them 14**](#_Toc179803123)

[**6.2.1 Establishing Objectives 14**](#_Toc179803124)

[**6.2.2 Monitoring and Communication 14**](#_Toc179803125)

[**6.2.3 Documentation 14**](#_Toc179803126)

[**6.2.4 Planning for Achievement 15**](#_Toc179803127)

[**7. Supporting processes 16**](#_Toc179803128)

[**7.1 Resources 16**](#_Toc179803129)

[**7.2 Competence and Awareness 16**](#_Toc179803130)

[**7.2.1 Competence and training 17**](#_Toc179803131)

[**7.2.2 Awareness 17**](#_Toc179803132)

[**7.3 Communication 17**](#_Toc179803133)

[**7.4 Documented information 18**](#_Toc179803134)

[**7.4.1 General 18**](#_Toc179803135)

[**7.4.2 Creating and updating. 18**](#_Toc179803136)

[**7.4.3 Control of documented information 18**](#_Toc179803137)

[**8. Operations 20**](#_Toc179803138)

[**8.1 Operational Planning and Control 20**](#_Toc179803139)

[**8.2 Information Security risk assessment 20**](#_Toc179803140)

[**8.3 Information security risk treatment 20**](#_Toc179803141)

[**9. Performance evaluation 21**](#_Toc179803142)

[**9.1 Monitoring, measurement, analysis, and evaluation: 21**](#_Toc179803143)

[**9.2 Internal audit 23**](#_Toc179803144)

[**9.3 Management review 23**](#_Toc179803145)

[**10. Improvement 25**](#_Toc179803146)

[**10.1 Continual improvement 25**](#_Toc179803147)

[**10.2 Nonconformity and corrective action 25**](#_Toc179803148)

[**References 26**](#_Toc179803149)

# Introduction

This document is a comprehensive guide designed to assist organizations in implementing the ISO 27001:2022 standard, a globally recognized framework for information security management. ISO 27001:2022 lays the groundwork for creating a robust Information Security Management System (ISMS) that safeguards sensitive data, fosters a culture of security, and drives ongoing security improvement. The guide follows the ISO 27001:2022 structure, breaking down its sections to provide clear insights and practical steps for effective implementation. It covers critical elements such as ISMS scope, leadership and governance, risk assessment and treatment, resource management, operational control, performance evaluation, and continual improvement. By simplifying the ISO 27001:2022 standard and offering valuable best practices, this guide is a valuable resource for organizations at any stage of their information security journey, enhancing their security practices and compliance.

In essence, this document is your roadmap to successful ISO 27001:2022 implementation. It demystifies the standard, offering practical advice and step-by-step guidance to help you establish a robust ISMS that not only complies with requirements but also fortifies your information security defenses against potential threats and vulnerabilities. Whether you're a newcomer to ISO 27001 or seeking to refine your existing ISMS, this guide is your partner in achieving a higher level of information security and safeguarding your organization's sensitive data.

# Implementing the ISO 27001:2022 standard

1. Scope

Instead of referencing the scope of your ISMS, this phrase refers to the standard's scope. It outlines how the standard is a "one size fits all" document that is meant to be applicable across business sectors, nations, and organization sizes and may be used for several objectives [1].

## Normative references

Some standards are accompanied by additional documents that offer more details and are extremely helpful—if not necessary—for implementing the standard itself. The ISO/IEC 27000 standard, which defines the overview and language for an ISMS, is the one for ISO/IEC 27001 that is mentioned here [1].

## Terms and definitions

The reader is simply referred to ISO/IEC 27000 in ISO/IEC 27001, which is unlike many other standards, which contain no definitions at all [1]. This is the place to look if you feel the need to understand the precise definitions of some of the terms used in ISO/IEC 27001, albeit you may not always feel all that much wiser after reading the definition [1].

## The context of the organization and the scope of the ISMS

The clause focuses a strong emphasis on understanding the organization and its environment, making sure the ISMS applies to the company, and the necessity of a thorough understanding of the company's activities for its implementation [1]. The people in charge of implementing and managing the ISMS must be able to respond to inquiries regarding what the organization does, where it operates, how it operates, and for whom [1].

Relevant Toolkit documents:

• Information security Context, Requirements and Scope

### The context of the organization

Determining the organization's context, specifically:

* Both internal and external issues.
* The expectations of interested parties are both internal and external concerns.

The management review, which also must be documented, must consider context changes [1].

### The scope of the ISMS

The information security management system's scope may be ascertained from the context. The standard requests that we define it and give the reasons why it was selected since this might refer to the entire organization or just one department. These justifications must be based on context-specific internal or external issues, including the expectations of the involved parties [1].

A document describing the scope must include information that indicates where ISO/IEC 27001 standards and security controls are implemented, why a risk assessment is conducted, what data the organization intends to protect, and which technologies are used to handle this data [1].

The following should be in the scope description:

* Attributes of the products or services offered.
* Information that the organization wants to keep secure (this item will be required for risk identification)
* Any relevant processes, including those carried out by entities outside the scope, and interfaces between external and internal processes.
* The management system's organizational structure
* The IT network's technology and a high-level description (such as a drawing); the sites and locations covered by the scope.
* Main suppliers

The same document can describe both the context and the scope. The scope may include certain items that are only citations to other papers [1]s.

Particularly if the management system is a portion of an organization, its limits must also be specified.

The scope of the ISMS differs from the scope stated on the certificate (if one is present), which is often quite brief and merely lists the services offered by the organization and integrated into the management system. There should be further information in the ISMS scope document.

### Information security management system

According to the requirements of the standard, the organization must create, implement, maintain, and enhance an information security management system within the selected scope [1].

## Leadership

The term leadership is used in ISO/IEC 27001, as mandated by the HLS, to emphasize the role of senior management: not only providing support but also a model and a guide.

* Establishing an information security policy and ensuring that its objectives are in line with the organization's strategic direction [1].
* Other responsibilities include ensuring the availability of the resources required for the ISMS to function and communicating its importance through the appropriate channels.

The Board of Directors, the Managing Director, the General Manager, or the CEO are all obvious examples of top management in organizations where the management system's reach encompasses the entire organization [1].

Look for the money (Sutton's principle) to determine who holds a top management position when the scope only includes a portion of an organization. Top management is made up of those who determine how much money should be set aside for information security [1].

Relevant Toolkit documents:

• Information Security Management System Manual

• Information Security Roles, Responsibilities and Authorities

• Information Security Policy

• Executive Support Letter

• Meeting Minutes

### Information security policy

The statement should state:

* A framework for determining the information security goals, taking into consideration the organization's concept of "information security"; it's crucial for the organization to have unambiguous general guidelines to adhere to and broad strategic goals.
* The management's dedication to meeting the ISMS's standards and working to enhance it.

It is necessary to document the policy, disseminate it inside the company, and, if necessary, make it accessible to interested parties. Any sensitive information cannot be included in the policy if it is partially or entirely released outside of the organization [1].

### Roles and responsibilities

If required, top management must define and convey the first level's tasks and responsibilities, as well as any additional positions that the management system may require [1]. Every level of a hierarchy, in turn, needs to define the duties and obligations of the individuals it oversees.

## Planning

This pivotal stage serves as the blueprint for establishing, implementing, monitoring, and continuously improving information security practices within the organization. It encompasses essential components such as risk assessment, risk treatment, setting security objectives, and strategic planning. Through this stage, organizations not only identify potential vulnerabilities and threats but also craft a proactive and comprehensive strategy to safeguard sensitive information assets. Let's delve into the planning stage of ISO 27001 to understand how it forms the bedrock of an effective information security program [2].

Relevant Toolkit documents:

* Information Security Objectives and Plan
* Risk Assessment and Treatment Process
* Risk Assessment Report
* Risk Treatment Plan
* ISMS Change Process
* ISMS Change Log
* Asset-Based Risk Assessment and Treatment Tool
* Statement of Applicability
* Scenario-Based Risk Assessment and Treatment Tool
* Opportunity Assessment Tool

### Actions to address risks and opportunities

To ensure the information security management system can effectively achieve its intended outcomes, prevent, or mitigate undesired effects, and facilitate continual improvement, the organization must carefully identify and address relevant risks and opportunities. This involves planning actions to tackle these risks and opportunities and integrating them into the information security management system processes. Additionally, the organization should evaluate the effectiveness of these actions to ensure the system's ongoing enhancement [2].

#### Information security risk assessment

##### Establishing Risk Criteria

organizations must define and implement an information security risk assessment process. This process involves the creation and maintenance of specific information security risk criteria, encompassing both risk acceptance criteria and guidelines for conducting risk assessments.

##### Ensuring Consistency

The risk assessment process should guarantee that repetitive risk assessments yield results that are consistent, valid, and comparable over time, providing a reliable basis for decision-making and security improvements.

##### Identifying Risks

This phase involves applying the risk assessment process to identify information security risks associated with the potential loss of confidentiality, integrity, and availability of data within the scope of the information security management system. It also involves identifying the individuals or entities responsible for managing these risks.

##### Analyzing Risks

The analysis stage assesses the potential consequences of identified risks and evaluates the realistic likelihood of their occurrence. This analysis helps in determining the levels of risk, enabling organizations to prioritize their security efforts effectively.

##### Evaluating Risks

In the final step, the results of the risk analysis are compared with the established risk criteria. This evaluation aids in prioritizing the analyzed risks for subsequent risk treatment activities, ensuring that the most critical vulnerabilities are addressed promptly and effectively within the organization's information security framework.

#### Information security risk treatment

##### Selecting Treatment Options

Organizations must establish and apply an information security risk treatment process. This process involves the selection of suitable information security risk treatment options, taking into consideration the outcomes of the risk assessment.

##### Determining Necessary Controls

As part of the risk treatment process, organizations must identify all controls that are essential for implementing the chosen information security risk treatment option(s). These controls form a crucial part of the organization's security strategy.

##### Control Comparison

The complaint process requires organizations to carefully compare the controls identified above and ensure that no essential controls have been overlooked or omitted, guaranteeing comprehensive coverage of security measures.

##### Statement of Applicability

Within the risk treatment process, organizations should create a Statement of Applicability. This document includes the necessary controls, and their justification for inclusion, and specifies whether these controls are implemented or not. Additionally, it provides justifications for excluding any controls from the information security framework.

##### Risk Treatment Plan Formulation

Risk treatment process, organizations are tasked with developing an information security risk treatment plan. This plan outlines the specific actions and measures to be taken to mitigate or manage identified security risks effectively.

##### Approval and Acceptance

It is crucial to obtain the approval of risk owners for the information security risk treatment plan. Furthermore, organizations should ensure the acceptance of the residual information security risks, solidifying commitment to the proposed security measures and their impact on risk reduction.

### Information security objectives and planning to achieve them

#### Establishing Objectives

Set information security objectives that align with the organization's information security policy, are measurable when feasible, and consider applicable security requirements, as well as insights from risk assessments and treatments.

#### Monitoring and Communication

Ensure that these objectives are actively monitored, communicated throughout the organization, and updated when necessary.

1. Documentation

Maintain documented information about the established information security objectives.

#### Planning for Achievement

When plan resources achieve these objectives, determine what actions will be taken, identify the required resources, and assign responsibility to relevant individuals or teams.

By adhering to these principles, organizations can effectively set, manage, and work towards their information security objectives in accordance with ISO 27001 standards.

## Supporting processes

Relevant Toolkit documents:

• Information Security Competence Development Procedure

• Information Security Communication Program

• Procedure for the Control of Documented Information

• ISMS Documentation Log

• Information Security Competence Development Report

• Awareness Training Presentation

• Competence Development Questionnaire

### Resources

The resources necessary to build, implement, maintain, and improve the ISMS must be provided by the organizations.

Economic and physical resources (such as buildings, IT systems, and other infrastructure) are both resources. Resources also include both internal and external staff members [1].

Implementing this need should follow a PDCA cycle: identifying the resources required, locating them, assessing their sufficiency, and acting as necessary [1].

The requirement for the establishment of an economic budget management procedure to identify resources is implied in the standard.

### Competence and Awareness

It is not just internal personnel who must comply with the obligation.

Applying the PDCA cycle is crucial in this situation—it is implicitly mandated by the standard, particularly for competency management.

#### Competence and training

Technical prerequisites for competency include an understanding of ISO/IEC 27001, privacy laws, UNIX systems, Cisco firewalls, and secure programming guidelines.

#### Awareness

The following topics should be covered in awareness exercises at the very least:

* The information security policy
* How everyone may contribute to the efficiency of the information security management system (so that staff are adequately informed of relevant processes)
* The advantages of a successful ISMS
* The repercussions of failing to adhere to the ISMS's standards (to be handled in accordance with a defined disciplinary process)

### Communication

The organization should assess whether internal and external communications are necessary [1].

The organization needs to decide on the following for each sort of communication:

* Who has the power to communicate?
* What should be communicated?
* When should it be sent?
* Who are the internal and external stakeholders that the communication is intended for?

While it is not required to record every planned communication, it is nonetheless important to include details about them in the procedures that apply since they are an important element of the processes [1].

### Documented information

To be following ISO/IEC 27001, an organization must have information that is beneficial to its operations documented.

#### General

There were specifications for records and documents in the earlier edition of ISO/IEC 27001 and other standards [1]. The HLS established the idea of recorded information but failed to effectively differentiate between the two.

#### Creating and updating.

The organization must take the following steps to create, and update recorded information properly:

* Identification and details (such as a title, date, author, or reference number)
* Format (such as language, software version, graphics) and media (such as paper, electronic)
* Approval for appropriateness and sufficiency, review

#### Control of documented information

Information that must be documented to comply with this document's requirements and the information security management system must be regulated to guarantee [1]:

* It is accessible and usable when and where it is needed.
* It is sufficiently safeguarded.

The organization must take the following actions, as appropriate:

Distribution, access, retrieval, and usage; Storage and Preservation, including Legibility Preservation; Control of Changes (such as Version Control); and Retention and Disposal.

## Operations

Focuses on operational planning and carrying out previously defined procedures.

Toolkit document relevant to Operations:

* ISMS Process Interaction Overview

### Operational Planning and Control

Needs comprehensive process planning, carrying out the planned activities, and doing what is required to meet the goals. Necessitates the organization manage the intended changes; this is the same as keeping track of activities and evaluating how successful they are [1].

In order to plan and carry out measures that can reduce any negative impacts, it also requires that the implications of unintentional changes be examined. This is equal to managing nonconformities and corrective actions [1].

Identifying, agreeing upon, and controlling outsourced operations is necessary even if it is relevant to establishing a management system.

### Information Security risk assessment

Documenting the selected risk assessment strategy is one of the basic criteria. Identification, analysis, and assessment steps make up this procedure [1].

### Information security risk treatment

The outcome of this procedure should be a risk treatment plan with the selected treatments for each risk, with the findings of the risk assessment serving as inputs.

## Performance evaluation

Performance evaluation focuses on monitoring, measuring, analyzing, evaluating, internal audits, and managing reviews.

Toolkit documents relevant to performance evaluation:

* Process for Monitoring, Measurement, Analysis and Evaluation
* Procedure for Internal Audits
* Internal Audit Plan
* Internal Audit Program
* Internal Audit Checklist
* Internal Audit Report
* Internal Audit Action Plan

### Monitoring, measurement, analysis, and evaluation:

Monitoring and measuring people is not necessary because the emphasis is on processes and controls [1]. This does not prevent a company from conducting assessments of worker efficiency and capability, as well as potential technical or hierarchical career routes [1].

Monitoring:

According to ISO/IEC 27000, Monitoring means, system, process, or activity status determination [1]. Not only the technological systems but also processes should be monitored. This can be accomplished either through direct observation or, if practicable, with the use of automated techniques [1]. Event detection for IT systems is an example tool for monitoring.

Measurements:

According to ISO/IEC 27000, measurement is the process to determine the value. Measurements are frequently performed using spreadsheets or automated systems [1].

The requirements of the standard are:

* repeatability of the measurements: measurement results must be consistent under identical conditions [1].
* comparability of measurements: measurements taken at various times must permit the identification of trends or changes [1].

Few measurements are effective when it comes to information security. These include:

* The amount of time systems and their parts are unavailable [1].
* The time it takes to resolve an incident depends on its seriousness [1].
* Degree of risk [1].

Measurements are helpful to have since they can assist managers in making decisions [1].

According to the PDCA cycle, the monitoring and measurement process outlined in the standard includes the following steps:

* Plan:
  + - Identify what needs to be monitored and measured and consequently the variables or status to measure [1].
    - parameter comparisons (acceptability criteria, behavior patterns, certain instances) [1].
    - Monitoring and measuring techniques to guarantee consistent results and accuracy to the desired degree [1].
    - Various ways to display findings.
    - Frequencies for reviewing and assessing the findings, and those responsible for acting in such a manner.
* Do: Gathering of data as expected.
* Check: Examining and studying (judging) a situation in order to determine its significance.
* Act: Selecting and implementing effects in order to address certain events.

Depending on the goals of the company, it is feasible to modify the status to monitor, the variables to measure, the data collection techniques, and the assessment criteria when the PDCA cycle is repeated [1].

### Internal audit

An audit program must be prepared to identify what areas to be audited. The scope for the ISMS and required time for the audit necessary to be identified since the audit process must be systematic [1]. Depending on the scale of the organization, auditing is conducted yearly or divided into multiple years.

When conducting an audit, it is necessary for the auditor to confirm that the agreement and internal procedures are followed for performing supplier audits. Auditors must obtain audit evidence by reviewing documents and records, interacting with relevant parties, and paying attention to the tools used.

The internal audit objective is to determine whether each employee complies with ISO/IEC 27001 and company procedures.

The results of the audit must be communicated to higher hierarchical levels, such as top management, as well as managers of the audited departments [1]. It can be required to update the audit program at the conclusion of each audit in order to make it better [1].

### Management review

The standard mandates that management evaluates the following,

* The status of the initiatives and plans set forth in the last review [1].
* Contextual changes from the last assessment, both internal and external, are relevant to information security [1].
* Results of monitoring and measurements relevant to the managers attending the review [1].
* Results of internal audits or external audits [1].
* Interested parties’ feedback [1].

A report must include the management review and any relevant findings. The standard requires management review at "planned intervals" [1]. The frequency should be at least once a year and be related to the organization's entire budgeting procedure [1]. When major changes take place, it may often be desirable to do additional, rare, or more frequent partial reviews [1].

## Improvement

Develop and handle remedial measures, and ongoing progress as well as nonconformities.

Relevant Toolkit documents:

• ISMS Process Interaction Overview

### Continual improvement

The organization must constantly improve the information security management system's suitability, sufficiency, and effectiveness.

### Nonconformity and corrective action

Nonconformity is a requirement that was partially satisfied. Corrective action is an activity taken to get rid of a nonconformity's cause and prevent it from happening again [1].

When one or more nonconformities occur, they can be examined to ascertain the reasons behind them and whether any corrective measures can be taken to prevent future occurrences. The ISMS may need to be modified because of such actions [1].

Additionally, after doing an initial study for some nonconformities, the organization may decide against taking any further action due to the associated costs or potential harm to information security.

All remedial measures must be documented along with any corresponding nonconformities, completed analyses, follow-up plans, and the findings of the final effectiveness assessment. If necessary, an improvement registry may be used [1].

# References

|  |  |
| --- | --- |
| [1] | "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#. |
| [2] | ISO/IEC, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," *Third edition 2022-10,* 2022. |