Sri Lanka Institute of Information Technology

ISO 27001 Implementation for Stark Industries

ß

IE3102-Enterprise Standards for Information Security

Submitted by:

Student Registration Number	Student Name
IT20250560	Rajapaksha R.M.P.S

Date of submission:

29th September 2021

TABLE OF CONTENTS

ABSTRACT

The importance of data protection and integrity preservation is at the topmost of priorities for any organization. Although there are many ways in achieving the security of that information, how it is implemented makes a huge difference in how it performs in the real world. The procedures that need to be followed should be done so according to a proper plan in order to avoid any inconveniences. Therefore, after a good amount of research I managed to come up with a number of steps in order to mitigate potential threats to information security if followed and implemented effectively. Also, I have identified currently existing international standards for serving such purposes. When combined with each other they will serve the purpose of information security well.

INTRODUCTION

One of your organization's most significant assets is information. The goals of information security are to preserve information's confidentiality, integrity, and availability of organizational information [1]. These fundamental principles of information security contribute to an organization's ability to protect itself against various types of threats and attacks, such as,

- Both mistakenly and on purpose, sensitive or secret information is given away, spilled, or improperly exposed.
- A breach of personally identifiable information
- Without the organization's awareness, crucial information is mistakenly or purposely updated.
- Critical business information is lost with no trace or possibility of recovery
- Important business information is unavailable when needed.

Due to that such threats, all managers, information system owners or custodians, and users, in general, should be responsible for ensuring that their information is effectively managed and safeguarded against the diversity of risks and threats that any organization faces.

Organizations can use the ISO/IEC 27001:2017, Information security management systems - Requirements standards as a foundation to create an efficient information security management framework for managing and protecting their crucial business assets, while minimizing risks, maximizing investment and business opportunities, and ensuring their information systems remain available and functional [1].

This is a major international standard for information security and is formally known as ISO/IEC 27001. It was published in 2013 by the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), and it was made accessible to the public at that time (IEC) [2]. The general structure changed in 2019.

ISO 27001 strongly encourages the adoption of an information security management system (ISMS) [2]. This strategy aims to combine information security with a cohesive management system to establish a unified set of controls, which many rapidly expanding organizations may initially lack. Because ISO 27001 examines assets that aren't always tied to information technology, this standard appears more accessible to a broader range of enterprises, but ISO/IEC 27001 standard mainly be used for third-party accreditation of information security management systems (ISMS). An authorized certification body audits the ISMS of organizations that want accredited certification. This guarantees that they have adequate management procedures and systems in place that meet the criteria of ISO/IEC 27001.

The final goal of this standard is to provide a risk-focused enterprise management system that is compatible with any type of information asset protection. It can protect information assets held in IT systems, on hard copy or digital media, and even in people's heads.

SIGNIFICANCE OF THE TOPIC

• Importance of having ISO/IEC 27001

Every company makes, stores, and disseminates information, and all of it is valuable. Implementing an internationally renowned information security management system is a nobrainer for protecting the company's assets and creating a significant return on investment [3]. Among the potential benefits are,

- Capability to operate in regulated marketplaces that need demonstrable data protection.
- Having that formal accreditation to utilize as a selling factor when seeking new consumers
- Operational expenses can be minimized by decreasing information security management processes and focusing on security controls where they are most needed to avoid big attacks.
- Cutting the cost of responding to information and cyber incidents is a top objective.
- There is more proof of conformity with rules and regulations, and the punishments for violating them are less severe.

ISO/IEC 27001 provides guidance on implementing ISMS control standards and assessing existing control implementations to assist organizations in preparing for ISO/IEC 27001 certification. The whole ISO/IEC 27001 documentation can be divided into two parts. Such as,

- Clauses 4-10

Specify the criteria for procedures in an ISMS. Which describes how an organization should set up and manage its ISMS. A company that wishes to earn ISO/IEC 27001 certification must meet all of these standards; exceptions are not permitted.

- Annex A

Contains a list of ISMS controls. The ISO/IEC 27001, Annex A, ISMS controls are not mandatory. They are meant to be used as an aide-memoire to help the organization in detecting where it may have overlooked a risk or applicable security control during its risk assessment and risk treatment plan development. ISO/IEC 27002 goes into further depth about these controls.

Figure 1

• Requirements

The core requirements of the standard are addressed in Clauses 4.1 through 10.2 [4].

4.1 – Understanding the Organization and organizational Context

4.2 – Understanding the Needs and Expectations of Interested Parties

4.3 – Determining the Scope of the Information Security Management System

4.4 – Information Security Management System

5.1 – Leadership & Commitment

5.2 – Information Security Policy

5.3 – Organizational Roles, Responsibilities & Authorities

6.1 – Actions to Address Risks and Opportunities

6.2 – Information Security Objectives & Planning to Achieve them

7.1 – Resources

7.2 – Competence

7.3 – Awareness

7.4 – Communication

7.5 – Documented Information

8.1 – Operational Planning & Control

8.2 – Information Security Risk Assessment

8.3 – Information Security Risk Treatment

9.1 – Monitoring, Measurement, Analysis, and Evaluation

9.2 – Internal Audit

9.3 – Management Review

10.1 – Nonconformity and Corrective Action

10.2 – Continual Improvement

- **Implementation**

Various IT efforts can save implementation time and cost [3]. As previously said, a business must also have a thorough grasp of the PDCA implementation phases in order to control project expenses. The PDCA cycle, which is compatible with all auditable international standards, requires an organization to take the following PDCA steps:

Step 1: Form an Implementation Team.

The first order of business is to choose a project manager to oversee the ISMS installation. They must understand information security and be able to direct and make decisions for others (whose departments they will need to review).

The project manager must enlist the help of others. Upper management can hand-pick the team or give the team's leader the freedom to put together their own group. After forming the team, they should develop a project mandate. These are basically responses to the following questions:

- What do we mean by success?
- Please provide a time frame.
- How much money can we expect to spend? • Is top management on board with the project?

Step 2: Create an Implementation Strategy.

The next phase is to put up the infrastructure for the implementation. The charter will be used to establish the implementation team's information security vision, strategy, and threat inventory.

To do this, we must first define the ISMS's guiding concepts, such as those that:

- Carry out various duties
- Directions for the concept's future development.
- Techniques for disseminating information about the effort both within and beyond the firm.

Step 3: Launch the ISMS

When the plan is finished, it is time to choose an improvement strategy. ISO 27001, although not requiring a specific technique, does advocate for a "process approach." Essentially, a PlanDoCheck-Act structure [3].

Any model may be utilized if the needs and processes are specified, effectively executed, and regularly assessed and improved [3]. Create a policy for the Information Security Management System as well. This isn't a comprehensive strategy, but it should define the implementation's goals and the measures that will be done to achieve them. After that, the board must grant its seal of approval. Now is the time to complete your paper layout. We recommend a four-pronged strategy, which includes:

Top-level rules outline the company's position on certain issues, such as allowed usage and password security [3].

- ways for carrying out the policies' provisions
- Procedures for carrying out duties in compliance with such policies.
- Documentation that adheres to specified standards and rules

Step 4: Define the ISMS Scope

The next stage is to examine the ISMS structure at a high level. This procedure is fully detailed in ISO 27001 clauses 4 and 5. This is an important phase since it defines the overarching aims of your ISMS and how it will affect your day-to-day operations. The ISMS must take into account the uniqueness of your firm in order to be effective.

The first order of business is to establish ISMS objectives. Tracking down the multiple computers and storage devices where information is stored is a part of this approach. If you want your ISMS implementation project to be a success, you must carefully determine its scope.

If you do not extend your emphasis, your company's data security may be threatened.

However, when the scope of the ISMS becomes too broad, it no longer fulfills its intended function.

Step 5: Identify the Security Baseline

An organization's security baseline is its basic minimum for secure operations. You may establish your organization's current level of security using the data from your ISO 27001 risk assessment. Using this strategy, you may home in on the most serious security flaws in your company and the associated ISO 27001 control to close them.

Step 6: Establish a Risk Management Process

The primary goal of an ISMS is risk management. Risk management is a critical ability for any firm wanting to adopt ISO 27001. This is because your security system is designed around the threats you've identified and prioritized. Businesses can use the Standard as a reference to design their own risk management procedures. Common techniques frequently focus on the possible risks to specific assets or the likelihood of certain outcomes.

Whatever approach you use, your decisions must be guided by a risk assessment. This method is broken down into five stages:

- Create a method for assessing possible hazards.
- Locate the dangers
- Examine the potential hazards carefully.
- Identify and analyze possible hazards; and
- Select a Risk Management Strategy.

Next, decide what type of risk you're prepared to take, taking into account the severity of probable consequences as well as the likelihood of unfavorable occurrences. For managers, the

higher the risk matrix score, the greater the hazard. They will then decide on an actionable risk level. A risk can be dealt with in one of four ways.

- Recognize and accept the threat
- Reduce risk by performing the following:
  - Avoid exposing yourself to the hazard in the first place.
  - The risk should be shared (with an insurance policy or via an agreement with other parties).

Finally, ISO 27001 requires enterprises to submit an SoA (Statement of Applicability) outlining which controls from the Standard were implemented and which were not, as well as the reasons behind those decisions [3].

Step 7: Implement a Risk Treatment Plan

When you apply the risk management strategy, you develop the security procedures that will secure your company's data. For the implementation of these measures to be effective, the staff's capacity to utilize and interact with the controls, as well as their understanding of their information security duties, must be validated [5]. You'll also want a process for identifying, assessing, and improving the skill sets required for ISMS success. To do this, a requirements analysis and identification of a target skill set are necessary.

Step 8: Measure, Monitor, and Review

It is hard to determine if your ISMS is effective unless it is evaluated on a regular basis. We recommend doing this at least once a year to maintain a close eye on the ever-changing risk landscape. The review process begins with the development of criteria that match the objectives you expressed at the start of the project mandate. A popular metric is a quantitative analysis, in which you assign a numerical value to the measured variable. This is important when utilizing resources that require either a monetary investment or a time commitment. Instead, employ qualitative analysis, in which decisions are based on expert opinion. When numerical grades such as "high," "medium," and "poor"

are insufficient, qualitative analysis is utilized. Furthermore, your ISMS should be subjected to regular internal audits.

Because ISO 27001 audits can be completed in any sequence, individual departments can be evaluated individually. As a result, you may avoid large production losses and ensure that your team is not overworked.

However, in order to obtain the findings, study them, and plan for next year's audit, you should endeavor to complete the procedure as quickly as possible. Your internal audit results will be used as inputs for a management review, which will then inform your organization's continuous improvement cycle [5].

Step 9: Certify the ISMS

The next choice is whether or not to pursue ISO 27001 certification, which calls for an evaluation of your ISMS by an outside party. The certification audit procedure is divided into two steps. The initial audit's main objective is to determine how closely the ISMS has been developed in compliance with the requirements of ISO 27001 Further investigation won't be done if the auditor isn't persuaded. You should be sure that you can complete the certification process before starting because it takes time, and you will still get paid if you do not succeed.

Another thing to consider is choosing a certification body. Consequently, the person auditing your system has to be aware of those demands. There are many choices, but you should confirm their validity by making sure they have been endorsed by a national certifying body that is a current IAF member (International Accreditation Body).

According to ISO 27001, the review will be carried out. In contrast, non-accredited businesses' claims of certification are false. It seems sense that you would want to save costs wherever you could, and the price of the certification audit will undoubtedly factor into that. The reviewer's past understanding of your particular field is another thing to consider. Since every

ISMS ever created has been customized to the unique requirements of the organization that created it, whomever is auditing your system must be knowledgeable about

ASSETS REGISTRY

Asset Register	
ABC Ltd.	
Version Number 1.0	Dt. 07.09.2009
Document Number	Asset Registory 001
Document Owner:	Stark Industries
Periodic Review:	Six Monthly
Last Review Date:	25/09/2022
Document Prepared by:	Dilshan K.N
Scope:	ISMS PROJECT
Audience:	Involved or related to ISMS PROJECT

Index

Figure 01

List of Digital assets and Valuation of Digital Assets

ABC Ltd.

Version Number 1.0 — Dt. 07.09.2009

#	Asset Title	Asset Details		Value
1	Database	Asset ID	1	9
		Owner	Stark Industries	
		Custodian	Stark Industries	
		Users	Employees, Executives, Managers	
		Location	192.168.122.1	
		Storage Details	Database	
		Classification	Internal	
		Life Cycle	Every 6 hours	
		Disposal Method	Delete of database records	
		Backup Schedule	Weekly	
		Backup Location	to databse backup server	
		Confidentiality Requirements		H
		Integrity Requirements		H
		Availability Requirements		H

List of Source Codes and Valuation of Source Codes

ABC Ltd.

Version Number 1.0 Dt. 07.09.2009

#	Source Code	Source Code Details		Value
1	Application	Asset ID	2	7
		Owner	Stark Industies	
		Custodian	Stark Industies	
		Users	Employees, Executives, Managers	
		Location	192.168.122.1	
		Procejt Manager	General Manager	
		Life Cycle	Internal	
		Business Specific requirements		
		Technical Contact	Admin	
		Version Number	v1.0.0.1	
		Expected Life	20 months	
		Expired Life	after 20 months	
		Maintenance Status	under maintaince	
		Purpose / Service / Role	Internal Employee	
		Dependency	yes	
		Backup Schedule	Weekly	
		Backup Location	backup server	
		Confidentiality Requirements		H
		Integrity Requirements		H
		Availability Requirements		L

List of Softwares and Valuation of Softwares

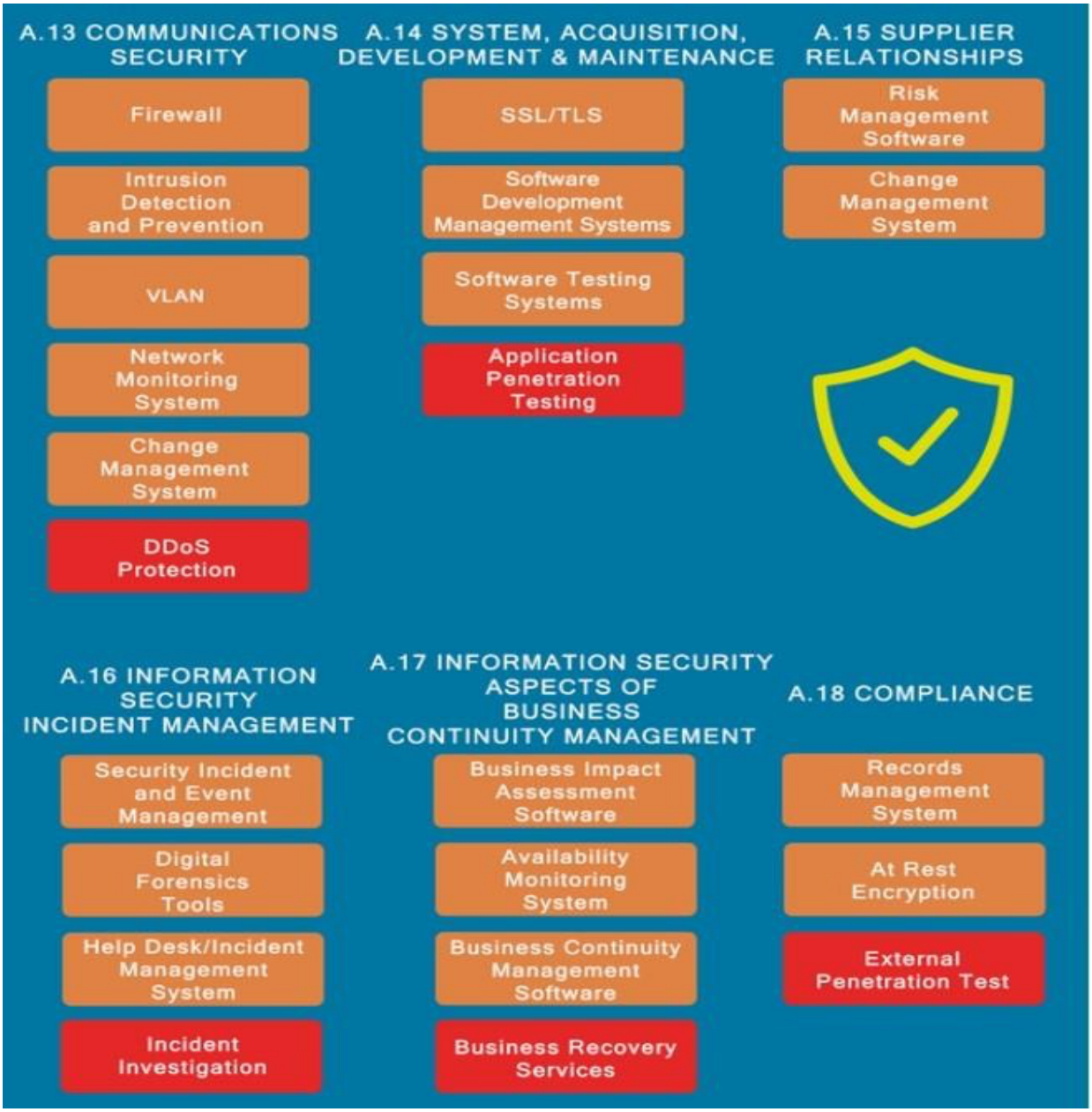
ABC Ltd.

Version Number 1.0 Dt. 07.09.2009

#	Description	Details		Value
	Bussiness Software	Version	RedHat Enterprice linux 8.6	3
		License Details		
		No. Of Licenses	1	
		Application / Business Specific requirements	continouse update	
		Technical Contact [SA/NA/DBA]	DBA	
		Vendor	RedHat	
		Expected Life	12 Months	
		Expired Life	After 12 months	
		Maintenance Status	Under Maintaince	
		Purpose / Service / Role	OS	
		Dependency	No	
		Redundency Requirenebts	Yes	
		Confidentiality Requirements for data Processed		L
		Integrity Requirements for data Processed		L
		Availability Requirements for data Processed		L

ASSOCIATED TOOLS


FOR THE ANNEX A CONTROLS
A.5 INFORMATION SECURITY POLICIES
Policy Communication and Testing
A.6 ORGANIZATION OF INFORMATION SECURITY
Mobile Device Management
Virtual Private Networks
A.7 HUMAN RESOURCES SECURITY
User Awareness Training
Phishing Penetration Testing
Verification Checking Services
A.8 ASSET MANAGEMENT
Data Classification
Data Loss Prevention
Secure Media Disposal Service
Secure Courier Services
A.9 ACCESS CONTROL
Password Management
Two Factor Authentication
Source Code Control Software
A.10 CRYPTOGRAPHY
Encryption Software
A.11 PHYSICAL AND ENVIRONMENTAL SECURITY
Access Control Systems
Alarm Systems
UPS and Generator
A.12 OPERATIONS SECURITY
Anti-Malware
Log Management
Vulnerability Scanning
Patch Management
File Integrity Monitoring
Change Management System
Performance and Capacity Monitoring System
Backup Management System


A.13 COMMUNICATIONS SECURITY
Firewall
Intrusion Detection and Prevention
VLAN
Network Monitoring System
Change Management System
DDoS Protection
A.14 SYSTEM, ACQUISITION, DEVELOPMENT & MAINTENANCE
SSL/TLS
Software Development Management Systems
Software Testing Systems
Application Penetration Testing
A.15 SUPPLIER RELATIONSHIPS
Risk Management Software
Change Management System
A.16 INFORMATION SECURITY INCIDENT MANAGEMENT
Security Incident and Event Management
Digital Forensics Tools
Help Desk/Incident Management System
Incident Investigation
A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
Business Impact Assessment Software
Availability Monitoring System
Business Continuity Management Software
Business Recovery Services
A.18 COMPLIANCE
Records Management System
At Rest Encryption
External Penetration Test

CONCLUSION

It has come to my understanding that by identifying the above international standards as well as following the afore mentioned steps it is possible to effectively maintain information security within an organization. It should also be maintained that the consistency and the functioning of each step individually and correlation with each other is crucial to function well. As information security threats evolve each minute the defense mechanisms should also be updated accordingly. In which case, sometimes certain steps may have to be altered to suit the relevant scenario. But in a vaster generalization of the applicability, I believe that the steps mentioned would prove to be effective as they are.

References

[1] Heru Susanto, Fahad Bin Muhaya, Mohammad Nabil Almunawar, and Yong Chee Tuan, *Refinement of Strategy and Technology Domains STOPE View on ISO 27001,* Vols. 1-1, no. Cornell University Library, p. 7, 2010.

[2] MARK EVANS, YING HE, CUNJIN LUO, IRYNA YEVSEYEVA, and HELGE JANICKE, *Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique,* Vols. 2-3, no. IEEE, p. 30, 2019.

[3] I. J. ARCHIVES, "Planning for and Implementing ISO 27001," ISACA JOURNAL ARCHIVES, 01 July 2011. [Online]. Available: https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-forandimplementing-iso-27001. [Accessed 16 September 2022].

[4] Alliantist Ltd, "ISO 27001 Requirements," Alliantist Ltd, 2022. [Online]. Available: https://www.isms.online/iso-27001/requirements/. [Accessed 19 September 2022].

[5] D. Kosutic, "ISO 27001 checklist: 16 steps for a successful ISO 27001 implementation," Advisera Expert Solutions Ltd, 2022. [Online]. Available: https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/. [Accessed 21 September 2022].