International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Analysis of ISO/IEC 27001:2013-Information Security Management System in an Organization

Dr. C. Sunitha [a], *Ranjana R* [b]

[a] *Associate Professor and Head, Department of Software Systems, Sri Krishna Arts and Science College, Coimbatore, India*
[b] *IV M.Sc SS, Department of Software Systems, Sri Krishna Arts and Science College, Coimbatore, India*

DOI: https://doi.org/10.55248/gengpi.4.1023.102841

ABSTRACT

Misuse of information can result in the unwanted revelation of private and business information, harming the company's reputation and the trust of the stakeholders, suppliers, and third parties who invest in that company. It is the responsibility of the organization to maintain its data. Companies facing data breaches frequently are the result of poor data security systems. Therefore, the security improvement program is contained in the Information Security Management System (ISMS). ISMS is developed with ISO 27001 standard certification. ISO 27001 is a standard that contains security management system requirements issued by the (ISO) International Organization for Standardization and IEC (International Electro-technical Commission) for establishing, implementing, maintaining and continually improving an information security management system. The standard ISO/IEC 27001 focuses on the security of the information. The information security management system provides a broader framework for all types of assets. The study aims to specify the methodology to perform risk assessments and treatments based on the gap analysis. The assessment of the security controls will result in the improvement of the effective and successful implementation of ISO/IEC 27001-2013.

Keywords: ISO 27001, ISMS (2013), Risk Assessment, Risk Treatment, GAP Analysis, Security Controls.

1. Introduction

Information misuse can result in the unwanted revelation of private or business information, harming the company's reputation and reducing business volume. Information security protection has grown more crucial as a result of the need for many firms in the globalization era to enhance data security to inspire public confidence in the investments and pledges made. The ISO 27001 certification for information security management systems is given in response to the requirement for information technology and security management in business.

Most businesses in the European Union utilize the ISO 27001 standard, according to (2017) data. The ISO 27001 standard enables enterprises to quickly respond to regulatory requirements established by the European Union, such as GDPR (2019), as well as security requirements that are beginning to be requested by their customers or other stakeholders. An objective benchmark for assessing organizational information security and preventing data breaches is provided by ISO 27001 accreditation. It compiles, organizes, and offers a set of specific regulations based on best practices (ISO, 2022). The ISO 27001 standard is regarded as a precise and useful information security management instrument in actual operation.

For firms, integrating information security into their corporate cultures and business operations appears to provide clear benefits. It appears that the investments in an information security program will pay off if information security is integrated with all business activities. The ISO framework is a collection of standards that can be used by enterprises to safeguard their information methodically and economically through the implementation of an Information Security Management System (ISMS).

The study on ISO/IEC 27001 contains what should be done for organizations that want to implement and build an effective security management system that explains how to conduct a series of activities that are specific to an organization. Though ISO 27001 has been implemented since 2005, there are still complaints from stakeholders, and third parties regarding the security of the information. It aims to quantify the effectiveness of security controls and their maturity level based on the observation through a practical audit.

2. Literature Review

2.1 Definition of ISO/IEC 27001

Standard 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies the conditions for the use of information security controls that are tailored to the needs of specific organizations or subsets thereof. Any business, regardless of form, size, or nature, may utilize this standard.

2.2 Information security management system ISO/IEC 27001-2013

An ISMS is a set of policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS guarantees the confidentiality, availability, and integrity of information using a systematic method for establishing, implementing, running, monitoring, reviewing, maintaining, and enhancing information security inside an organization. Based on an organization's risk acceptance levels and risk assessment, ISMS effectively addresses and manages risks. The successful deployment of an ISMS depends on the analysis and the application of appropriate controls to ensure the security of these information assets, when necessary.

It involves the application and management of appropriate controls that include consideration of a wide range of threats, intending to ensure sustained business success and continuity and minimizing consequences of information security incidents.

2.3 Risk management

The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review.

Iterative approaches to risk assessment and treatment are possible in the information security risk management process. Performing risk assessments iteratively leads to the assessment's depth and detailing. It strikes a fair mix between reducing the time and effort required to establish controls while guaranteeing that high risks are properly addressed. The context is established first. Then, a risk assessment and treatment is conducted. Another risk assessment iteration with altered context iteration is necessary if the information is insufficient.

2.4 ISO 27001 risk assessment & treatment – six steps

a) ISO 27001 risk assessment methodology

The first step through risk management in ISO 27001 is to define the rules to perform risk management and to make the whole organization do it the same. The biggest problem with risk assessment that happens in the organization is by performing it in different ways. Therefore, qualitative or quantitative risk assessment must be defined with scales for qualitative assessment, what the acceptable level of risk will be, etc.

b) Risk assessment implementation

Organizations are usually aware of only 30% of their risks. Therefore, once you know the rules, list all the assets, then threats and vulnerabilities related to those assets, assess the impact and likelihood for each combination of assets/threats/vulnerabilities, and finally calculate the level of risk.

c) Risk treatment implementation

The implementation of the risk treatment in ISO 27001 is to mitigate each unacceptable risk as not all risks are created equal, therefore it is to focus on the most important one, called the ‘unacceptable risks’.

d) Risk Assessment and Treatment Report

Assessment and treatment need to be documented in everything done so far. It includes the auditors and personnel to check those results in a year or twice.

e) Statement of Applicability

This document shows the security profile of an organization– based on the results of the risk treatment in ISO 27001 and the implementation of all controls. Therefore, this document is very important as the certification auditor uses it as the main guideline for the audit.

f) Risk Treatment Plan

The purpose of the Risk Treatment Plan is to define exactly who is going to implement each control, in which timeframe, with what budget, etc. Therefore, the document is called an ‘Implementation Plan’ or an ‘Action Plan’.

3. Implementation Roadmap

The design and development of information systems frequently overlook information security. Therefore, information security is often thought of as being a technical solution. This operates successfully and efficiently, it recognizes and controls a variety of operations. Any resource-intensive activity must be managed to enable the conversion of inputs into outputs through a series of connected or cooperating activities; the output from one process can serve as the input to another, and this conversion is typically carried out under planned and regulated circumstances. A "process approach" can be used to describe the implementation of a system of processes within an organization, as well as the identification, relationships, and management of these processes. The processes undertaken are as follows:

- ✓ Understanding the changes
- ✓ Assessing training requirements
- ✓ Performing a Gap Analysis on existing controls
- ✓ Revisiting Risk Assessment
- ✓ Updating Risk Treatment Plan (RTP)
- ✓ Updating Statement of Applicability (SOA)
- ✓ Booking transition audit
- ✓ Implementing any changes
- ✓ Promoting ISO 27001 certification
- ✓ Focusing on continual improvement

4. Gap Analysis

An ISO 27001 gap analysis provides a high-position overview of what needs to be done to achieve the instrument and enables you to assess and compare the association's information security arrangements against the conditions of ISO 27001. It measures the current state of compliance against the Standard and enables you to compass your ISMS parameters across all business functions. The first step of this tool is to develop a gap analysis roster that serves to identify gaps between spoken procedures and processes performed. This checklist is grounded on the requirements of ISO 2700- 2013.

4.1 Checklist Assessment

Checklist Assessment by repliers grounded on current organizational conditions. The repliers chosen were the ones who had enough capability. Assessments were made under the scoring conditions.

4.2 Gap Assessment

Gap assessment aims to watch how big the gap in the company is. The chance value is attained by casting the score per variable and dividing it by the maximum value in that variable. The lower the gap is, the better the result.

5. Result and Analysis

5.1 Analysis of ISO/IEC 27001 Clauses 4 to 10

4. Analysis of Context of the Organization Clause

The organizational clause of 27001 is to determine the internal and external issues, and requirements of the interested parties to achieve the intended outcomes. The purpose is to adapt ISMS to determine the scope and to enable and manage risks associated.

5. Analysis of Leadership Clause

The Leadership clause of 27001 acts to cover the overall responsibility that directs and controls the organization to demonstrate leadership, commitments, policies, roles and responsibilities concerning ISMS by the top management.

6. Analysis of Planning Clause

The Planning clause accounts to determine the risks and opportunities that provide the key to Information Security Risk Assessment, its vulnerabilities and a risk treatment plan (ASMR) based on the Annex A controls of ISO 27001.

7. Analysis of Support Clause

The Support clause is to provide and analyze the resources, the competence of the personnel, awareness and communication plans of what, why, whom and how, and regular defining of security objectives, policies, and controls that lead to the success rate of ISMS.

8. Analysis of Operational Clause

The Operational clause need to address the plans, implementations and control the processes including the risk assessments and treatments at planned intervals in the minds of the top management.

9. Analysis of Performance Evaluation Clause

The Performance Evaluation clause of ISO 27001 shall monitor, measure and evaluate to address the risks and the security performance by conducted by internal audits at the organization during planned intervals.

10. Analysis of Improvement Clause

The Improvement clause states that the organization to conduct work on the continual improvement based on the complaints from the parties, stakeholders customers etc. It should address the non-conformities according to (RIIE) cycle.

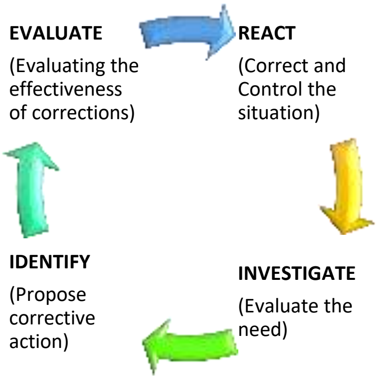

EVALUATE
(Evaluating the effectiveness of corrections)
REACT
(Correct and Control the situation)
IDENTIFY
(Propose corrective action)
INVESTIGATE
(Evaluate the need)

Fig 1- RIIE Cycle

5.2 Analysis of Annex A Controls

Table 1 and Fig 2 below are based on the practical evaluation with the key stakeholders, reviewing technical documentation and checking readiness to conduct ISO/IEC 2700-2013 certification.

The important step of the assessment was the evaluation with the stakeholders and employees to collect information and check on the current control set and the risks.

Conformity level	Description
Major Non-Conformity	Significant improvement needed
Minor Non- Conformity	Minor to moderate improvement needed
Conforms	No improvement needed

Table 1-Maturity Level of ISO 27001-2013

Since most of the organizations implement the 2013 version of ISO/IEC 27001, the subsequent pages include the observations and recommendations based on a review of the current state of ISMS capabilities for improvements needed to achieve the level of maturity required for ISO 27001 certification.

A.5.1 Management direction for information security

Observation

The Standard Operating Procedures (SOPs) covering different industry domains are described in logical and physical Security SOPs. The policy is being reviewed immediately on special request and is reviewed annually.

Conformity Level

Major Non-Conformity

Recommendation

It recommends information security policy into topic-specific policies, to further mandate the implementation of information security controls that are typically structured to address the needs of certain targets like cryptographic controls, antivirus controls, mobile devices and teleworking, management of technical vulnerabilities etc.

A.6.1 Internal Organization

Observation

- Enforcement of Information Security policies is being established and managed by top management. The security strategies are approved by the directors of respective IT, production, PMO, quality assurance and compliance.
- Instructions related to the workflow is managed by the HR department. The ideology direction of procedures, implementation and adherence of policies is concurrently managed by the QA, compliance and IT directors.
- Based on the assessment the Information Security event/incidents are investigated internally and identifying contact with relevant authorities is not established.

Conformity Level

Minor Non-Conformity

Recommendation

It recommends to appointing compliant personnel for each policy who then becomes responsible for its day-to-day implementation.

A.6.2 Mobile devices and teleworking

Observation

- Policies for the conditions and restrictions for the use of teleworking haven't been defined.
- The general check of anti-virus and automatic software updates are turned on for both corporate and private businesses. E-mail templates with the requirements for laptops and new employees are being managed by the IT department.
- Remote working connecting to VPN networks with credentials are allowed for the employees.
- No policy for usage of public Wi-Fi, BYOD is documented.

Conformity Level

Major Non-Conformity

Recommendation

To implement a policy named Teleworking policy to ensure that teleworking is undertaken safely from an information security perspective that describes teleworking activities, acceptable use of information processing facilities, guidelines for the use of public Wi-Fi and prohibited activities.

A.7.1 Prior to employment

Observation

- Background checking policies/procedures are used.
- Employment screening, terms and conditions are adapted.
- Contracts specifying NDAs and confidentiality clauses are signed by the employers, stakeholders, suppliers, etc.

Conformity Level

Conforms

Recommendation

N/A.

A.7.2 During employment

Observation

- Overall conducting of security awareness/training is being regularized. The safe working process of employees is carried out through audits.
- E-mails regarding the general advices for the best work practices and information security incidents concerning its violation are sent by the respective management.
- Disciplinary process describing violation activities is not documented either in conditions of NDA or in IT security.

Conformity Level

Major Non-Conformity

Recommendation

To implement a Security Awareness policy that defines the scope, procedures, topics, roles and responsibilities in terms of the awareness program. It should also document and implement disciplinary processes that are designed to provide a structured corrective action process to improve and prevent a recurrence of undesirable employee behaviour and performance issues.

A.8.1 Responsibility for assets

Observation

- Inventorization of access cards and assets with information issued to the employees is carried out with detailed descriptions to the owner by the IT department.
- Policies for the use of technology resources (browser extension, etc.) for the organization's asset on any employee's termination are lacking by the organization at some point.

Conformity Level

Major Non-Conformity

Recommendation

To document and implement a formal policy and procedures for acceptable use of applications, hardware, information and other information technology resources and systems which establishes assets inventory and methods of inventory either conducted manually or with the help of automatic tools.

A.8.2 Information Classification

Observation

- The organization lacks policies/procedures covering the handling of assets for digital classification of information.
- Procedures for labeling information are documented.

Conformity Level

Major Non-Conformity

Recommendation

To add procedures describing the classification of digital information which aims to ensure that information is handled according to the risk or impact to ensure the CIA (Confidentiality, Integrity and Availability) triad of data.

A.8.3 Media handling

Observation

No proper procedures for the regulation and removal of removable devices (USB drives, hard disks, etc.) are described.

Conformity Level

Major Non-Conformity

Recommendation

It recommends to documenting and implementing procedures to create a Removable Media Policy that would prohibit or allow acceptable usage of USB flash memory or external hard drives, define roles and responsibilities to minimize the risk of loss or exposure of sensitive information maintained by client and reduce the risk of acquiring malware infections on computers.

A.9.1 Business requirements for access control

Observation

Procedures for Access Control within logical and physical security are described. Access to network-related services (VPN, Wi-Fi) is documented.

Conformity Level

Minor Non-Conformity

Recommendation

It recommends establishing Access control procedures in a separate policy that defines who may access the services describing the logical access conditions to those services by the intended authorities.

A.9.2 User access management

Observation

- No procedures for regulating employee’s privileged access rights are described.
- Permissions on projects are led by project managers and team leads.

Conformity Level

Minor Non-Conformity

Recommendation

The assessment recommends limiting a certain number of rights via creating a new organizational unit (OU) instead of Active Directory users’ local admin rights. Organizational Units must add procedures that would describe the removal or adjustment of access rights during changes of employment.

A.9.3 User responsibilities

Observation

Procedures requiring the usage of password managers from the employees are not documented.

Conformity Level

Major Non-Conformity

Recommendation

To document and implement a policy that outlines the need for well-thought-out password protection (e.g. usage of password managers).

A.9.4 System and application access control

Observation

- Though the employees have MFA configured to their G-mail accounts, no procedures for enabling MFA for the version control system are documented.
- No procedures were established restricting the use of system utilities.

Conformity Level

Major Non-Conformity

Recommendation

Usage and documentation of Multi-factor authentication is highly encouraged whenever possible, not only for work-related accounts but personal accounts.

A.10.1 Cryptographic controls

Observation

- Neither a documented policy framework nor related controls on the use of cryptographic controls were established.
- Rules defining Full Disk Encryption usage and key management process procedures are not regularized.

Conformity Level

Major Non-Conformity

Recommendation

- To establish a cryptographic controls policy for the use of encryption techniques to protect sensitive data. To assign roles and responsibilities for:
    1. The implementation of the policy;
    2. The key management, including key generation.
- To develop and implement policies or procedures to create, manage, distribute, use, store, and revoke cryptographic keys and digital certificates.

A.11.1 Secure areas

Observation

- Surveillance cameras on entry, exits, confidential rooms and floors are installed.
- Physical log is implemented and maintained.
- Confidential papers are maintained in a locked room with a record of alert being played. The central alert system is configured for informal disasters.

Conformity Level

Minor Non-Conformity

Recommendation

Recommends installing an electronic logging of each employee to ensure that only authorized personnel are allowed access to certain organization premises.

A.11.2 Equipment

Observation

- Equipment is equipped with access cards, fire and security alarms, AC systems, surveillance cameras and UPS for power failures.
- Equipment maintenance outside the organization is not documented.
- Verification of equipment before the disposal of sensitive data is not performed.

Conformity Level

Major Non-Conformity

Recommendation

It recommends to documenting and establishing correct equipment maintenance outside the organization premises that enables full disk encryption, a clean desk policy to remove an end user workspace when not in use and secure disposal procedures in disposing and reusing sensitive data.

A.12.1 Operational procedures and responsibilities

Observation

- Operational procedures are defined and documented selectively.
- Software, Document and Contractual change control are regulated by the change management SOP. Test procedures are adopted and developed by the organization.
- Capacity management is represented through an Excel table with hardware models for the current state, no policy of capacity projections for plans is described.

Conformity Level

Minor Non-Conformity

Recommendation

Creating and documenting capacity projections describing the purchase plan and a comprehensive description of the separation of development, testing and operational environments is recommended.

A.12.2 Protection from malware

Observation

Anti-virus procedures regulating protection against malicious code have been adopted. Workstations run with Windows Defender Anti-virus.

Conformity Level

Major Non-Conformity

Recommendation

A policy describing malware protection is to be established. A precautionary control to install and update malware detection and scanning of web pages, files and e-mails over the network to be regulated on a routine basis.

A.12.3 Backup

Observation

- Backup process policy describing requirements to backup procedures according to classified type of information is regulated.
- Inactive projects on GitHub and GitLab are reviewed.
- Regular execution of backup recovery, testing procedures and instructions for execution are not defined.

Conformity Level

Minor Non-Conformity

Recommendation

It is recommended to implement and document procedures for regular testing of backup media to be relied upon in case of emergencies. Testing restoration procedures promptly is required.

A.12.4 Logging and monitoring

Observation

- Events of modification of network equipment and log-on activities are maintained by embedded functionality of network devices.
- No formal policy regulating the types of log-in organization is maintained and monitored. Responsibilities of key process and log retention periods are not defined.

Conformity Level

Major Non-Conformity

Recommendation

Documenting, implementing, and maintaining effective log management policies or procedures throughout the organization is recommended.

A.12.5 Control of operational software

Observation

- General recommendations describing not to install software that is not related to work are sent by the IT department.
- Installation of local operating systems software is not properly controlled by the organization.

Conformity Level

Major Non-Conformity

Recommendation

To develop, implement and detect procedures/controls for approving software installation and to implement preventive technical controls to restrict users' possibility to install software on operating systems is recommended.

A.12.6 Technical vulnerability management

Observation

- Vulnerability management control procedures for Unix-based server and user software have not been implemented.
- Policy defining roles, responsibilities, timelines and procedures within vulnerability within the management process has not been implemented.

Conformity Level

Major Non-Conformity

Recommendation

Vulnerability Management Policy establishing procedures for identifying and remediating vulnerabilities to minimize security breaches associated with unpatched vulnerabilities to be documented and implemented.

A.13.1 Network security management

Observation

- Segmentation of the network is implemented and divided into DMN, guest networks and internal network. Users working in guest networks where access from other networks is restricted.
- MAC filtering for internal wired and wireless connection has been established in Excel form.
- Despite the implementation of network controls no formal documentation is established.

Conformity Level

Minor Non-Conformity

Recommendation

Recommends to create formal documentation of network controls configuration.

A.13.2 Information transfer

Observation

- Neither documented framework procedures nor information transfer controls ensuring protection against unauthorized access, or misuse during transfer is established.
- NDA agreements are signed with employees and third parties but documentation of transfer of secret authentication information is not established.

Conformity Level

Major Non-Conformity

Recommendation

To establish, document and implement policy/guidelines that lay methods for the transfer of information and electronic messages that make users aware of what seems acceptable and what is not.

A.14.1 Security requirements of information systems

Observation

Information Security controls within the organization for new Information Systems to the existing systems are not included in the business requirements of change management policy.

Conformity Level

Major Non-Conformity

Recommendation

Defining requirements for new information systems to existing information systems within Change Management policy. The usage of secure authentication methods for applications accessible via public networks e.g. using public key cryptography, digital signatures and multifactor authentication to reduce the risks is recommended to be documented.

A.14.2 Security in development and support processes

Observation

- Initiation, analysis, design, development, testing, reporting, maintenance and activation are described in the Software Development Life Cycle policy. The policy states the project objectives, stakeholders, milestones, deliverables, roles and responsibilities, resources, risks, assumptions and constraints, high-level scope and requirements as initial steps.
- Software Change Control under the change management policy stands for formal change, test and release controls in the development lifecycle within the organization
- Neither documented procedures in the Project Initiation policy describing how risks should be determined nor identification of any risks of service delivery within outsourced software development has been adopted.
- Description of security testing procedures is lacking.

Conformity Level

Minor Non-Conformity

Recommendation

- To integrate Security Testing procedures.
- To document, apply and implement procedures defining Static analysis, Dynamic analysis, Fuzz testing, software design and software architecture.
- To conduct penetration testing procedures on software releases and to document and apply the Secure Coding Practices Checklist is recommended based on the Observation.

A.15.1 Information security in supplier relationships

Observation

Devices are purchased from authorized distributors and activate Microsoft Windows operating systems with regular license keys. Services of local laptop repair companies are purchased by the organization.

Conformity Level

Minor Non-Conformity

Recommendation

Identification of the types of suppliers to whom the organization allows access information must be documented based on the organization’s business needs and requirements. Enabling Full Disk Encryption (FDE) on laptops is recommended.

A.16.1 Management of information security incident and improvements

Observation

- Policy regulating responsibilities and the procedures in terms of information security incidents management process hasn’t been adopted by the organization.
- Policies/procedures regulating reporting of information security incidents and weaknesses, learning from information security incidents and collecting evidence are not formally documented.

Conformity Level

Major Non-Conformity

Recommendation

- Establishing and maintaining responsibilities to follow procedures listed below are developed and communicated adequately.
    1. Incident response planning and preparation.
    2. Monitoring, detecting, analysing and reporting Information Security events/incidents.
    3. Forensic evidence.
- To build an Information Security Incident Response Team (ISIRT) to support reporting actions, help reporting persons and make them aware the employees of events including
    1. Human errors and non-compliance.
    2. Breach issue of CIA triad.
    3. Malfunctions and access violations of software/hardware are recommended.

A.17.1 Information security continuity

Observation

- The organization has a business continuity and Disaster Recovery policy containing an Emergency Management Team, Data and Systems Recovery Timing and Disaster Recovery Activities. Scenarios for mitigation of emergency are defined and adopted.
- An additional reserve switch is installed in a server rack for protection against network failure.
- Virtual machines in VMware are configured to auto start after a power outage and are audited by the IT department once per quartal.

Conformity Level

Minor Non-Conformity

Recommendation

To integrate verification of information security continuity controls regularly with the organization's business continuity plans to ensure that they remain up-to-date and effective.

A.17.2 Redundancies

Observation

Information processing facilities are protected from power failures and other disruptions by UPS, redundant heating/ventilation and air-conditioning systems.

Conformity Level

Conforms

Recommendation

It is recommended to test redundant information systems to ensure the failover from one component to another component works as intended.

A.18.1 Compliance with legal and contractual requirements

Observation

- Personal Data processing agreements are signed by the employees with their clients. Admin inventory, an unlicensed tool to monitor and control Microsoft Active Directory users and other unlicensed/outdated workstations run in versions of Microsoft Windows OS is used.
- Data protection policy contains a responsible person for managing internal data protection activities and a classification matrix to protect Personally Identifiable Information (PII).
- Neither documented framework nor related controls identifying any risks of regulation of cryptographic controls were established.

Conformity Level

Minor Non-Conformity

Recommendation

- For organizations conducting business in other countries, managers should consider compliance legislation in all relevant countries.
- Guidelines to be considered to protect any intellectual property:
    1. To publish an intellectual property rights compliance policy defining the legal use of software and information products.
    2. To acquire software only through reputable sources, carrying out reviews that only authorized software and licensed products are installed.
- To document guidelines on the retention, schedule, storage, handling and disposal of records and information.
- To the persons involved in the processing of Personally Identifiable Information (PII) should be communicated with the data protection policy.

A.18.2 Information security reviews

Observation

- SOPs of the organization are reviewed annually. The periodic independent review of opportunities for improvement and the need for changes to the approach to security are not processed by the clients.
- The compliance of information protection performed by NIST, HIPAA and GDPR standards and regulations relies on the organization's data protection policy.
- Procedures describing a regular review of technical compliance with the organization's information security policies and standards are not documented.

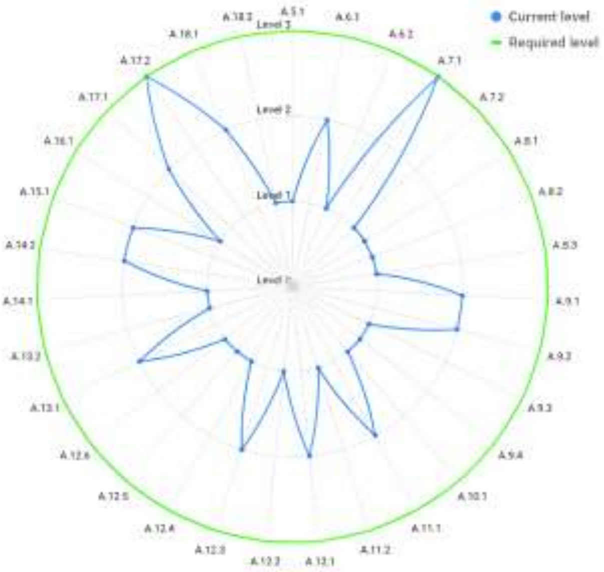
Conformity Level

Major Non-Conformity

Recommendation

- Initiation of an independent review of control objectives, controls, policies, processes and procedures for information security at planned intervals when significant changes occur is recommended.
- To review the compliance of information processing and procedures within each manager's area of responsibility, hardware and software controls with the appropriate security policies, standards and any other security requirements. As a result of any non-compliance, the managers should:

    1. To identify the causes of the non-compliance and evaluate the need for actions to achieve compliance
    2. To implement appropriate corrective action and review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.
    3. Penetration testing and vulnerability assessments to be carried out by independent experts should be planned, documented and repeatable.



Level 1 -Major Non-Conformity
Level 2 - Minor Non-Conformity
Level 3 – Conforms

Fig 2-Radar representation of the current maturity level of Annex A controls.

Conclusion

After the analysis of ISO/IEC 27001, it is evident that it provided a comprehensive approach to managing the information security of the organization. The core requirements of the clauses focus on identifying the needs and interests, focusing on the scope of the ISMS (clause 4), defining roles and responsibilities to establish policies (clause 5), assessing risks and vulnerabilities to improve information security (clause 6), defining and documenting the resources for maintenance (clause 7), defining risk treatment plans for implanting controls (clause 8), monitoring measuring and assessing the effectiveness (clause 9), and finally making corrective actions based on the non-conformities (clause 10). It primarily provided a framework for managing its risks and assets aligning the information security efforts with a continuous improvement. The assessment report of security controls provided a recommendation as a solution for the improvement of information security. The control group is the baseline for the ISO/IEC 27001 certification. However, baseline security is attained through careful planning and with significant resources. Therefore, the study demonstrates that the organization can successfully implement ISMS, significantly enhancing the organization's information security and providing stakeholders and third parties with confidence in the security of their data.

References

G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," Journal of Information Security, vol. 4, p. 92, 2013.

H Berg, "Risk management: procedures methods and experiences", Rt & a, vol. 1, no. 17, pp. 79-95, 2010.Nicho, M. A process model for implementing information systems security governance. Inf. Comput. Secur. 2018, 26, 10–38.

Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. J. Inf. Secur. 2013, 4, 92–100.

Cannon L., et al.: Certified Information Systems Auditor;Wiley Publishing, Inc., Indianapolis, Indiana, ISBN-13:978-0-7821-4438-3, pages 49-82.

Eloff, J.: Information Security Management - A newParadigma; Proceedings of SAICSIT 2003, Pages 130-136.

Aksorn, Thanet & Hadikusumo, B. H. W. (2007). Gap Analysis Approach forConstruction Safety Program Improvement.Journal of Construction in DevelopingCountries.Vol.12,No. 1.

W. Boehmer, "Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001", Proceeding of Second International Conference on Emerging Security Information Systems and Technologies, pp. 224-31, 2008.

Sennewald, C.A., Effective Security Management4th edition, Burlington, Elsevier Science, 2003.

Klaic, A. (2006). Information Security Requirements and the Information Systems Planning Process, .17th IIS Conference. (P. 265-269).

H Berg, "Risk management: procedures methods and experiences", Rt & a, vol. 1, no. 17, pp. 79-95, 2010.