International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1282-1288 www.ijaem.net ISSN: 2395-5252

Implementation of ISO 27001:2013 ISMS in a Defence Lab: A Case Study

[1,2] Shahela(JRF),Suchitra.G(JRF), [3]B Beulah Aswini (To'B'), [4]Pramod Kumar Jha (Sc'F'),

Centre For Advanced systems, DRDO, Hyderabad, Telangana
Centre For Advanced systems, DRDO, Hyderabad, Telangana
Centre For Advanced systems, DRDO, Hyderabad, Telangana
Corresponding Author: Pramod Kumar Jha

Submitted: 15-04-2022 Revised: 27-04-2022 Accepted: 30-04-2022

A
BSTRACT: In this digital age, Protection of data, information and intellectual property is crucial for any organization. In order to mitigate any security attacks, information systems need to be protected both physically and logically. Any information security threat like information theft, Denial of Service (DoS) and unauthorized access can cause an adverse impact on the corporate either by loss of revenue, reputation and trust from the customer/stakeholders. Implementing Information Security Management System (ISMS) can help to identify, manage and reduce any information security threats in the organization to a great extent. One of the widely accepted information security standards today is ISO/IEC 27001.This standard was developed for protection of information in ICT (Information and Communications Technology) and it includes generic methods and guidelines to address both security and privacy aspects of an organization.

This paper discusses the ISMS framework that is specifically designed for our organization to manage the three triad of information security namely aspects of confidentiality, integrity, and availability of data. It is an implementation of process, and technology concepts in protecting information security of the organization. An organisation by being certified in ISO 27001 ISMS, gives a lot of confidence to top management about information security best practices and their readiness to thwart any information security breaches.

KEYWORDS: Information Security, ISMS, ISO/IEC 27000 Series, Risk Assessment, Auditing, Confidentiality, Non-Conformity.

I. INTRODUCTION

The International Standard ISO 27001 is implemented in an organization for establishing, implementing, maintaining and for continuous improvement of an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's vision, mission, security requirements, and foremost the top management's commitment to enforce the system. The information security management system maintains the confidentiality, integrity and availability of the information by doing a risk management process, ensuring the interested parties that risks are managed well.

It is crucial that the information security management system is to be integrated with the organization's processes and complete management structure. It is also considered to strategize the processes, information systems, and controls. It is anticipated that an information security management system implementation will ascend in accordance with the needs of the organization. This international standard can be used by any parties to assess the organization's ability to meet the organization's own information security requirements.

II. IMPLEMENTATION METHODOLOGY

Implementation plan is one of the foremost activities, which helps to identify the activities, which needs to be performed to achieve the requirements of the standard. It starts with "As-is" analysis which helps to understand the existing system in place and to find the gaps in the system. Identified gaps are then filled with the required changes or enhancement in the system. The entire

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1282-1288 www.ijaem.net ISSN: 2395-5252

process can be performed with the help of Deming's famous PDCA (Plan-Do-Check-Act) cycle ISO 27001 has 10 clauses, from clause 4.0 to clause 10.0 and Annexure A, The Annexure A consists of 14 domains and 114 controls in it from A5 to A18.
ISO 27001,if examined by a PDCA cycle, gives a better vision to carry out the command and affiliate with improved business objectives.

2.1 PDCA Model - In ISO 27001
The PDCA Model was described by William Edward Deming in 1920, abbreviated as Plan, Do, Check and Act.
Plan: Clause 4 - Context of organization, Clause 5-Leadership, Clause 6-Planning, Clause 7-Support
Here planning for the organization ISMS compliance is checked by scheduling Internal and external Audits
Do : Clause 8 - Operations
Check : Clause 9 - Performance evaluation
Act : Clause 10 - Improvement

ISO 27001 ISMS implementation is a six-step process as stated below which are covered under the clauses and controls mentioned below.
1. Formulation of Security Policy
2. ISMS Scope definition
3. Assessment of Risks
4. Management of identified risks
5. Selection of Control objectives and implementation of controls
6. Preparation of Scope of Applicability (SoA).

Clause 1, 2 ,3 covers the general part as the type of organization, purpose of standard, requirements of organization, normative references, the terms and definitions which are earlier explained in ISO 27000 standard.

For an organization to begin, the Clause 4 to Clause10 are essential.

Clause 4– Context of the Organization
This includes understanding the needs and expectations of interested parties. The scope of the ISMS is defined in terms of the characteristics of the organization, assets and technology. It takes into account the interfaces with other systems, organizations and third party suppliers.
This standard specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the environment in which it operates in the organization. The requirements presented in this standard are general and are intended to be relevant to all organizations, regardless of size, type or nature.
Information asset is any item, property, or information, which has value to the organization. It can be a tangible asset (inventory, equipment) and intangible asset (patent, copyright, user rights).
Firstly, we have identified the information assets in our organization of each and every department and then classified them.
It supports the enhancement of IT infrastructure, which acts as a catalyst for ISMS implementation.
Clause 5-Leadership
It is the engagement of top management, promoting the ISMS.
The planning, awareness and sensitization of information is a paramount for achieving the ISMS certification.
Clause 6- Planning
To plan and continually reduce the organization's exposure to risk.
We have constituted an internal audit team which conducts ISMS audits twice in a year.
External audit from headquarters is conducted once in a year. Apart from the audits, we have in-house vulnerability assessment and penetration testing tools. An external audit for vigilance is also conducted every year.
The observations, which are the outcomes of the audit, are corrected and nonconformities are closed.
As per security policy, measurable objectives were established at relevant functions and levels. We have maintained a table of key performance indicators versus target.

The following are the key performance indicators implemented:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1282-1288 www.ijaem.net ISSN: 2395-5252

Sl.	Key Performance Indicator	Target
1.	Information security incidents	Nil
2.	Information security awareness-promotion programs	Once in 3 months
3.	Training and development-Man days	½ Man day/year
4.	Compliance to statutory and regulatory requirements	100%
5.	Mock drills-BCP	One in 6 months
6.	Information security surprise checks/inspection	One in 6 months
7.	Downtime %	5%
8.	Number of persons given awareness training	40

Table 1. Information security objectives

Clause 7-Support

The support we obtained is in terms of resources like capable infrastructure, equipment, competent right skill manpower, training and process to streamline, monitor and document it.

The support of industry partners, IT systems to increase the system reliability plays a major role in ensuring the system availability.

The evaluation of effectiveness of training and retaining documented information related to competence is done and finding the necessary competence of persons working under organization's control that affects its information security performance and ensures that these persons are competent on the basis of appropriate education, training, skills or experience.

The documented information is controlled to ensure it is available for authorised use as and when needed and is adequately protected.

While control of documented information is maintained and retained by the organization, the following are considered as applicable; Distribution, access, retrieval and use, Storage and preservation, including preservation of legibility, Control of changes (revision/issue), Retention and disposition.

Clause 8-Operations

This relates to implementing the actions to address risks and Information security objectives.

Risk management is the process of identifying the risk associated with every asset, then assessing the risk and controlling it.

Information security risk assessment is performed at least once in a year. The results of the information security risk assessments are confined by the Information Security Officer.

The information security risk treatment plan was done and determination of additional controls were placed in case of the risk values higher than the acceptable value.

Our organization has established the processes, documents and provided resources specific to the service for achieving the desired results. It has carried out required verification, monitoring and test activities related to the product.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1282-1288 www.ijaem.net ISSN: 2395-5252

Clause 9-Performance Evaluation

It can be done in 3 ways:

1. Effectiveness of ISMS is monitored
2. Internal & External audits are conducted.
3. Check that management reviews are happening and written down.

Organization evaluates the information security performance and the effectiveness of the information security management system and for this, it determines what is to be monitored; including information security processes and controls;

Internal audits are conducted once in 6 months to provide information on whether the quality management system conforms to the organization's own requirements.

An audit program (Plan & Schedule) is planned based on the importance of the processes concerned, changes affecting the organization, and the results of previous audits. The audit criteria, scope, frequency and methods and other details of conducting Internal Audit are described in the process or in the documented information (the internal audit plan, agenda, checklist, Non Conformity (NC)).

Clause 10-Improvement

It includes the corrective actions and the root cause analysis. This standard calls for continuous improvement and corrective actions to be taken after paper identification of root cause analysis. Standard techniques like 5 Why analysis is being used for this purpose.

In case of occurrence of a nonconformity, the organization takes action to control and correct it and deals with the consequences by reviewing and analysing the nonconformities determining their causes and if similar nonconformities exist, or could potentially occur. Based on the above actions, the organization makes changes to its ISMS, if necessary.

III. EXECUTION OF ISMS AT OUR ORGANIZATION

3.1 ISMS policy

- Ensuring that all information is treated with complete confidentiality and maintains its integrity and availability.
- Complying with all applicable requirements and continual improvement of information security management system.
- Safeguarding security of our information assets through effective business continuity management.
- Establishing information security objectives and reviewing the same periodically.

This Information Security Policy is communicated to all the persons within the organization and is made available to relevant interested parties.

3.2 Statement of Applicability (SoA)

As per clause 6.1.3, we have produced a statement of Applicability that contains the necessary controls and justifications for inclusions and exclusions in our organisation. This provides the overall process that is implemented/followed in our organization. SoA is applicable to all systems and information infrastructure being used in our organisation and its associated agencies wherever digital form of data is processed, stored and transmitted.

3.3 Internal Training

According to clause 7.3, ISMS training was conducted to the employees of the organization, to give them awareness of the ISMS policy, procedures and the controls. A quiz was conducted on ISMS for all the employees of the organization. Information Security Management related videos and documentation were uploaded in our intranet portal of the organization. Thus, we have provided complete knowledge on the ISMS ISO 27001:2013. This is a continuous everyday process wherein Cyber Security related tips are displayed in three official languages at various kiosk across the lab.

3.4 Best Practices implemented in our Organization

According to the 114 controls of 14 domains of ISO 27001, the best practices implemented are hereby mentioned below

A.5 – Information Security policy

Information Security Policy is placed at various work centers and intranet portals.

A.6 – Organization of Information Security

Information Security roles and responsibilities are explained, Role based Segregation of duties, Contact with authorities for communication, Contact with Audit groups for checking up NC's, Mobile device and Teleworking policy is implemented.

A.7– Human Resource security

Background verification of all permanent and contract employees is done.

Terms & conditions of employment are enforced.

Providing continuous ISMS awareness training and quizzes to all employees.

A.8 – Asset Management

We identify the organizational assets and prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

The count and list of assets is very important for proper health monitoring. The typical assets of an organisation are given in the bar chart below.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1282-1288 www.ijaem.net ISSN: 2395-5252

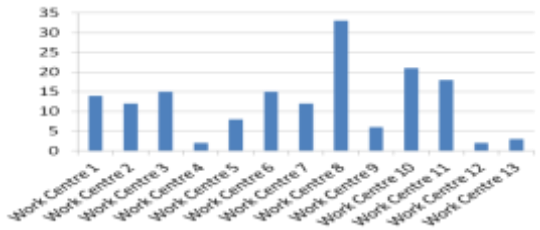

Fig.1 Number of Assets in CAS

A.9 – Access control

Information should be available to each and every authorised user so biometric based two factor authentication is necessary for endpoint internet systems.

The user accounts are created i.e., cloud and internal mail for accessing intranet systems with proper traceability of information access.

A.10 - Cryptography

All critical information exchange between various labs is done through an end-to-end encrypted communication platform such as internal cloud.

A.11 – Physical and Environment security

There is a proper baggage scanning, a valid access card entry, and frisking to avoid untoward entry in / out of the lab and also key management is implemented.

A.12 –Operations security

Under the operations, we have the RAID (Redundant Array of Independent Disk) configuration with auto backup of data for data redundancy. The test data is secured on non-internet servers.

A regular in-house tool based infosec audit is done with quarterly internal audits of work centres and an end-point security policy. Continuous upgradation and patch management of software's is done.

The firewalls are configured for both Internet and Intranet. UTM (Unified threat management) device is used to mitigate the risk from malware adware & control the social media websites.

A ISG (Information Security Gateway) firewall for Intranet is used, where in the default policy supports only encrypted packets from the external world.

An air gap between the internet and intranet is maintained at all times and only white listed pen drives are used for transfer of data.

A.13 – Communication security

For communication with the external world, only official email ids are used such as gov.in emails with two-factor authentication. Secure data exchange happens between functions and workcenters of organisations using private cloud and internal mails as shown in fig 2.

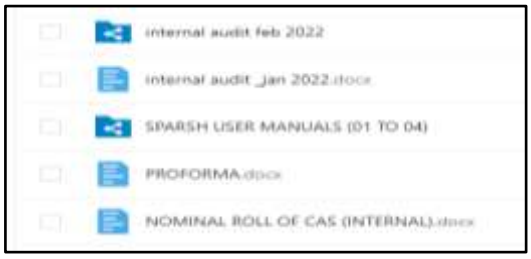

Fig.2 Internal cloud

In order to reduce the downtime and increase the efficiency, we implemented the IVRS (Interactive Voice Response System) for booking complaints which have the ticketing system and details of the number of complaints booked with a timely review of it as represented in below fig 3.

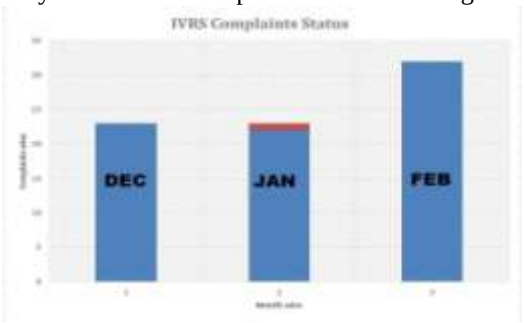

Fig.3 IVRS Complaint Booking

A.14 - System Acquisition, Development and Maintenance

To fulfil security requirements of Information Systems, which provide services over public networks, we are securing the information involved in application services on public networks from fraudulent activities.

Whenever operating platforms are changed, applications are reviewed and tested and restrictions are strictly applied on modifications to software packages.

A.15 - Supplier Relationships

In order to safeguard assets that are accessible by suppliers, the Non-disclosure agreement (NDA) is made with industry partners. A workable plan system is made to introduce the ISMS clauses as shown in fig.4.

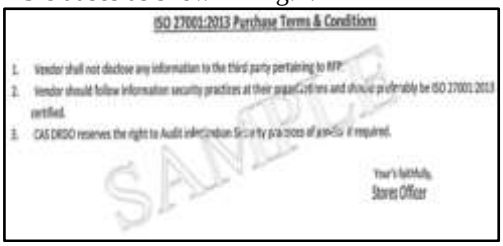

Fig.4 Sample of Supply Order of CAS

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1282-1288 www.ijaem.net ISSN: 2395-5252

A.16 – Information Security incident Management
The Information Security events are reported instantly through appropriate management channels and are recorded.
A.17 – Information Security Aspects of Business Continuity management
Defined disaster recovery procedures setting out responsibility channels of communication for execution staff and incorporated a distribution list for failure notification.
Two new clauses are incorporated in HR-NOC and supply order forms.
A.18 – Compliance
In internal audits, according to information security control 18.5, a form was introduced for maintenance schedules of IT infrastructure for NC's raised during internal audit were corrected and risks are mitigated.The IT risk register is updated to test data, security and storage.
Feedback form is introduced for the acknowledgement from employees of understanding the ISMS policies.
Role based access is given for IT tools.
Process for ISMS change management is corporated to document changes related to ISMS infrastructure.
Facility for updating secondary firewall as and when primary firewall is upgraded is incorporated so that the restoration can be done with minimum down time.
Log analysis of UTM devices are analysed periodically.
Tickets raised in IVRS are categorized according to priority so that complaints can be taken based on level of priority.
To-Do list is prepared in hindi and telugu for housekeeping and displayed regularly.
Mock drills including backup restoration are done once in six months to ensure readiness of departments.

3.5 Internal and External Audits:

ISMS Internal Audit at our organization

Internal Audits were conducted for every department functional within the organisation twice in a year. The findings and NC's of the audits were worked upon and closed.

3.6 ISMS External Audit at our organization

A two stage external audit was conducted by a third party organisation which visited all the departments of our organisation. The findings and observations were addressed. We have been certified from the certifying body.

IV. CONCLUSION

In our Organization, we are continuously evaluating processes and operations to conform to the standard by correcting the Non-Conformances (NCs) . raised by the audits.Improvements as suggested by the audits are incorporated to improve the system and meet the organisational objectives.

V. FUTURE SCOPE

Implementation of ISMS in a R&D organisation plays a vital role in safeguarding the critical information system and helps to create cyber awareness among the employees. This further helps to mitigate both internal as well as external risks. In future, we have to enhance the level of awareness among employees by conducting regular training,webinars, workshops and conferences in the areas of cyber security.

ACKNOWLEDGEMENT

The authors would like to thank Sri BV Papa Rao, Outstanding Scientist and Director, CAS for his constant support in implementation of information security best practices at CAS. Authors express their gratitude to Sri Praveen Tandon Sc G, Associate Director for his continuous encouragement throughout this implementation. Our thanks to the entire staff of the IT section,Internal Auditors for their untiring efforts towards achievement of this certification.The authors are touched by the generosity and expertise of all CAS employees which have contributed to this study in innumerable ways.

REFERENCES

[1]. DRDO Corporate information security policy document.
[2]. Protection of DRDO Data, DRDO Document..
[3]. DRDO Information Security Policy procedures and Guidelines,V3.0, DRDO Document.
[4]. https://ieeexplore.ieee.org/document/8471700
[5]. https://www.academia.edu/56641692/A_practical_implementation_of_ISMS
[6]. https://iopscience.iop.org/article/10.1088/1742-6596/1339/1/012103
[7]. https://www.drdo.gov.in/headquarter-directorates/area-of-work/information-technology-and-cyber-security
[8]. https://publications.drdo.gov.in/ojs/index.php/djlit
[9]. http://www.drdo.com/pub/techfocus/welcome3.htm

[10]. https://publications.drdo.gov.in/ojs/index.php/dsj
[11]. https://www.academia.edu/67190568/The_risk_assessment_and_treatment_approach_in_order_to_provide_lansecurity_based_on_isms_standard
[12]. https://bestpractice.biz/what-are-the-14-domains-of-iso-27001/
[13]. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained
[14]. https://egs.eccouncil.org/what-do-you-know-about-iso-27001/

CONTRIBUTORS

[1] **Smt Shahela** is presently working as a JRF at DRDO,CAS,Hyderabad.She completed her M.Tech in VLSI.She has published a paper on Quantum Circuitry in International Journal & Magazine of Engineering,Technology, Management and Research.She is certified as a ISO 27001 lead auditor.

[2] **Ms G.Suchitra** is presently working at DRDO, CAS, Hyderabad as a JRF. She completed her M.Tech in Computer Science & Engineering from Osmania University. She has 2 years of work experience in the field of computer science. She is certified as CISSP-Certified Information Systems Security Professional.

[3] **Smt B.Beulah Aswini** is currently working as a Technical Officer-B in DRDO,CAS, Hyderabad.. She has done her B.Tech degree in Computer Science & Engineering from JNTUH. She has more than 22 years of experience in the field of embedded systems and published research papers in DRDO IWD Journals on embedded systems. She is certified as an internal auditor on ISO 27001 She is currently working in the field of IT and Cyber Security.

[4] **Sri Pramod Kumar Jha,** Scientist-'F is presently working as a Technology Director, ITCS&AI at CAS DRDO Hyderabad. He has done his M Tech in Manufacturing Management from BITS Pilani. He has also obtained a couple of PG Diplomas and certifications in the areas of Operations and Project Management, Public Procurement etc. He has more than 22 years of research and techno-managerial experience in the areas of Real Time Simulations, Real Time Networks, Information Technology management and cyber security. He has published more than 20 research papers, articles and reports in various journals and conferences.