Best Practices of Auditing in an Organization using ISO 27001 Standard

Amogh Phirke, Jayshree Ghorpade-Aher

ABSTRACT— In recent year with the intensive use of the information technologies, data security has been turned into a critical and important issue in organizational management. Various Standard and rules are there for the security of Information, for example, ISO/IEC 27001, ISO/IEC 27002. However, organization face different challenges for implementing the standard. In this paper, we present the status of the ISO/IEC 27001 execution process in a Small and Medium Sized Enterprise. By executing ISO 27001, organization got the chance to prove authenticity and show the clients that the organization is working according to recognized best practices. It helped the organization "IKSC Knowledge Bridge Pvt Ltd." in reducing cost, risks, and increases the brand value. The outcomes obtained conclude not just the need to think about the technical, legal aspects of organization but also those related to people like training, knowledge, create awareness, to achieve a successful management of information security.

Keywords— ISO/IEC 27001:2013, Risk Mitigation, Software Audit, Controls, Compliances

1. INTRODUCTION

In upcoming era data security is one of the most important assets for IT industry. Risk Assessment is one of solution to prevent data from data theft and for recognizing loop holes in the organization that can cause security breaches. There should be a proper set of procedures and policies applied to prevent these security breaches to enter in to the organization. One of the framework which includes Risk Assessment is ISO 27001 Standard which deals with the overall security of the organization. This Standard starts from determining the scope of organization till certification of the Standard, although it is not mandatory that organization should be certified if the organization is following the mandatory policies and control to gain its objective. ISO 27001 Standard is used to implement Information Security Management System (ISMS) in an organization. Since the most of highest effect security breaches originate by employees working in the organization, there should to be a proper training in the organization to shield the system from being compromised internally, the awareness program should be conducted for the employees and staff so that the information security business continuity do not exclusively depends upon a specific individual presence which could lead to serious system halt/crash dependent on the accessibility of specific employees. Information Security Management System (ISMS) give a complete solution for a superior information security encounter by providing the needed procedures, tools, and measures for enhancing and maintaining a protected information organization [1]. The employees and staff of the organization should be given proper awareness and training about the ISO Standard and why it is important to their organization. After compliance with ISO 27001, the organization can give guarantee to their clients and partner that their data is secure within the organization.

2. LITERATURE REVIEW

Koldo Peciña and et al. used two techniques which is ISO 31000 and ISO 27001 resulting in both physical and Logical security evaluation. The only limitation was that there was no security management implemented to ensure protection of all assets. [1]. Carol Hsu and et al. compares the lists of firms with and without ISO 27001 certification with their performance. Only the Financial information was not available in any firm [2]. Manar Abu Talib and et.al. gives the importance of ISO 27001 procedure to execute in an information security management. The future scope was to evaluate the enriched Information Security course, and improve the Information Security Technologies [3]. Elvi Fetrina and et al. collected the data by interview and by literature study. The results of this survey is inventory management information. They used Rapid Application Development and Object Oriented Approach using Unified Modelling language. Problem regarding possibility of Loss or damage data arises in this case while implementing [4]. Awni Irtradat and et al. uses ISO 27001 which guarantee an ultimate protected environment for organization. The only limitation arises that the team who is implementing should have all the knowledge of ISO 27001 Standard [5]. Yogesh Verma and et al. highlights the design and development of a web based centralized software asset management systems, reduces the overall development cost, and improves the software value and efficiency. The limitation was that there was no monitoring and Evaluation for periodic built in feedback mechanism towards continuous improvement [6]. Martin Jakubicka, investigates the design of a Software Asset Management created for University purposes and addresses the most noteworthy issues in this situation. The only limitation was that there was no suitable methodology for creating SAM. Affifah Multiwina and et al. uses technique that manage their resources, maintain detailed asset record as well as maintain the conditions of the asset. The limitation was there was not much flexible assets [7]. Thomson Martin uses number of ways in which SAM can help an organization to keep assets safe but it takes a lot of
time, effort and support from Senior Management. The limitation was that it is not necessary that an expert in SAM may also be expert in Software Licensing. Viktor Shved and et al. proposed a technique that permits distinguishing executable documents assembled from a similar source code for different versions of systems and with minor changes to the source code [8].

3. PURPOSE OF THE INTERNAL AUDIT FOR ISO 27001 STANDARD

The purpose of audit is understanding with information security management system examining practices. The scope of the audit included an assessment of the information security services, forms, and controls portrayed within the ISMS documentation to secure the privacy, reliability and accessibility of the city’s critical information assets inside the scope of the ISMS. A list of twenty information resources was given at the beginning of the audit as the inventory to be considered within the scope of the ISMS.

4. IMPLEMENTATION OF ISO 27001 STANDARD

ISO/IEC 27001 gives regulating prerequisites to develop and operate in an ISMS, including a lot of controls for the controls and mitigation of the risks related with the information assets which the organization looks to protect by working its ISMS.

4.1 ISO 27001 Clauses

ISO/IEC 27001:2013 contains 10 clauses which are as follows:

- Clause 1 -Scope
- Clause 2 - Normative references
- Clause 3 - Terms and definitions
- Clause 4 - Context of the organisation
- Clause 5 - Leadership
- Clause 6 - Planning
- Clause 7 - Support
- Clause 8 - Operation
- Clause 9 - Performance Evaluation
- Clause 10 - Improvement

4.2 Steps for implementing ISO 27001 Standard in an organization

The ISMS might be certified as consistent with ISO/IEC 27001 by various authorize enlistment centers around the world. The ISO/IEC 27001 certification, as other ISO management system certifications, for the most part includes a three stage audit process:

PDCA is very important for implementation of the project.

The ISO/IEC 27001 Standard states that for implementing the standard following are the steps which is to be followed:

a. Defining the ISMS policy
b. Scope of the ISMS
c. Preparing for Risk Assessment
d. According to risk assessment and identified risk selection of controls which is to be applied
e. Preparation of Statement of Applicability

Stage 1 — Find out the Objective of the organization

The objective of the organization is obtained from the company’s mission and vision. The goal can be:

1. Assurance to the employees and client that they are fully compiled with the information security.
2. The data which is taken from the employees and client is protected.
3. Continues improvement in productivity of the organization.
4. Ethically running with IT guidelines.

Stage 2 — Get Organization Support

The organization should take guarantee that it will cooperate with the implementer while implementing the standard for improvement of the ISMS. Obligation must consolidate exercises, for instance, guaranteeing that the most potential resources are accessible to work with ISMS and that all deligates of the ISMS which are doing training.

Stage 3 — Characterize ISMS Scope

According to the ISO 27001 Framework, there are 114 controls, which are organized in 14 Domains and 35 control objectives organization, but the framework states that it is not mandatory to implement all the controls. It depends on the size of the organization and its objective. But it should be mentioned that why that control is not applicable to your organization. ISMS Scope must be specified in order to be get certified from external auditors[14].
Stage 4—Define risk assessment methodology

After studying and analysing objective and risk associated with the organization, we have to formulate a proper risk assessment methodology. The methodology should contain the proper treatment of risk which includes resolution and controlling of risks faced by the organization. We also have to identify and distinguish the resources from which the risk occurs and harm the organization security [14].

Stage 5—Prepare Risk Treatment Plan

After identifying the risk associated with the organization, probability and consequences of each risk is measures or analyze and drawn in the table. Depending on the probability and consequences of risk, priority of treatment of each risk is decided. Risk treatment plan includes basic risk mitigation strategic which includes accepting, avoiding, transferring or reducing the risk to a certain level of acceptance.

Stage 6—Developing ISMS Implementation Program

As mentioned in step 3, controls should be selected with respect to size of organization and the organization objectives. Not all the controls are mandatory to implement the ISMS framework. According to the objective of the organization among 114 controls specific controls which is needed to implement Information Security Management System [14].

Stage 7—Documentation of adopted controls in an organization.

For the controls applied, as mentioned in the SOA, the organization will require articulation of arrangement or a complete procedure strategies and report to recognize client role for reliable and execution of approaches and techniques.

List of documents and practices which is also called as Statement Of applicability (SOA) is mandatory document for certification of ISO 27001.

Stage 8—Reviewing of compliances

After implementing all the controls in the organization, it should be reviewed periodically whether the controls implemented in the organization suitable for the objective of the organization. Monitoring of objective, control, measurement methodologies comes together in this phase [14].

Stage 9—Preparing for Internal Audit

Sometimes the employee knowingly and unknowingly takes wrong discussion while achieving the objective of the organization, which leads to decrease in performance of the organization so it is important to perform an internal review. So corrective and preventive action is to be taken to meet the required objective [14].

Stage 10—Periodic Management Review

Periodic Management Review deals whether the implemented policies and procedures are being followed or not to achieve organization’s objective. This step is always important for taking action against the employee who are violating the policies and procedures [14].

5. RESULTS AND ANALYSIS

It’s a E-learning based institute. Previously, there was no ISMS policies and controls applied in an organization. There was lack in proper documentation and procedures in an organization due to which it was facing with many difficulties and internet threats. Even there was no supervision on network security. Firstly, we did the gap analysis and studied about the existing procedures and control applied in the organization. After doing the gap analysis we come to know that there are many mandatory processes and control which are good to have in an organization for network security purpose.

Firstly, we make a list of mandatory controls which is to be implemented from ISO 27001 Standard checklist. We get to know that there are many softwares used in organization so the handling and enhancing the purchase, deployment, maintenance, consumption, and removal of software is required in an organization. Along with this solution for Risk management, MIS reporting, disaster management was also required.

Along with this we also applied the policy to deleted unwanted data after a particular period of time, policy to alert when internet data allotted to each student exceeds, policy if data theft occurs, policy to block and check whether anyone is uploading files on dropbox and blocking the USB port to avoid altering of computer system and data theft along with policy to measure the productivity of each student is also applied. As information security becomes a public concern, certification would benefit the certified firms through competitive advantages. All these issues can be eliminated by implementing ISO 27001 Standard in an organization. Hence, we have studied about ISO 27001 and started with establishing ISMS Scope according to the requirement of an organization. Along with these, we also studied about different policies that is to be applied in organization, which will help to implement ISO, 27001 framework.

After implementing the project, we get to know that it helps the organization to save cost and time in Software Audit, IT related Configuration, overall management done by higher authority and IT effort done by network Administrator. The organization easily do monitoring of all the assets (which also includes human) and softwares installed in the systems. After implementing the Standard, the organization can easily check the productivity of each student on daily basis as well as on monthly/yearly basis. This comes under Human Resource Management which can help business to gain a competitive advantage.

Fig. 3. Reduction in Time Activity Graph.
6. CONCLUSION

As information security becomes a public concern, ISO 27001 certification on information security management system (ISMS) would benefit the certified firms through competitive advantages. All these issues can be eliminated by implementing ISO 27001 Standard in an organization. Hence, we have studied about ISO 27001 and implemented the ISO 27001 framework according to the requirement of an organization. Along with these, we also studied about different policies that is applied in organization, which will help company to protect from security threats and helps to increase its productivity.

REFERENCES

5. Elvi Fetrina, Eri Rustomaji, Tatat Nuraini , Yusuf Durrachman, “Inventory Management Information System Development at Bprtiik Kemkominfo Jakarta”, IEEE 5th International Conference on Cyber and IT Service Management (CITSM), 8-10 August 2017


