ISSN: 1832-5505

Applied GIS

Vol-7 Issue-02 April 2019

Using the ISO 27001 Standard for Risk Analysis in Software Compliances

Amoghi Phirkei [1], Jayshreei Ghorpade-Aheri [2]

MIT Engineering and World Peace University

***Abstract*—** Data is one of a company's most valuable assets. It is crucial to have a reliable and protected Information System in order to have access to the company's data. Data confidentiality, integrity, and accessibility are all essential features of a safe system. The solution to these problems is data security, which entails conducting a security audit of the system in order to identify, assess, and rank the threats to the information assets of IT systems. In order to differentiate risks and their impact on the business, a risk assessment technique has been established. Based on the results of the vulnerability analysis, a risk assessment is developed for individual data assets. The ISMS that an organization adopts has as its primary focus the protection of its data and computer systems.By conducting a case study centered on the business in question, this report provides an evaluation of the state of information security there. The purpose of this case study is to demonstrate how vulnerabilities assessment and penetration testing may be used to identify threats to an organization's information systems from both the legislative and technological perspectives, and then arranged into a risk assessment strategy. In order to eliminate threats to the organization's information systems, an Information Security Management System (ISMS) compliant with ISO/IEC 27001:2013 was established throughout the course of the case study. The ISMS provides the necessary controls and measures to restrict the identified risks and to permit the examination and improvement of an organization's information security.

***Keywords*—** *Assessment of Risk, Conformance, and Controls According to ISO/IEC 27001.2013*

INTRODUCTION

Hackers are increasingly targeting organizations in an effort to get access to private data for nefarious ends, such as financial gain, identity theft, and political motive. Damages from cyberattacks may extend beyond the monetary costs of repairing infrastructure after a breach and the legal risks associated with such an event. Thus, the focus for administrators and technology assets must shift from responding to cyber security incidents after they occur to developing a plan and system to identify and neutralize cyber threats before they have an impact on the business. While there are many other sorts of Cyber-attacks, phishing, ransomware, and insider risks from malevolent clients have all been seen to be on the rise.

In the 21st century, information is seen as a crucial resource by every company. Assessing a system's susceptibility to attack is called a vulnerability assessment, and it helps pinpoint weak points in information security by singling out the threats that pose the most danger to an organization's resources. To identify and differentiate security holes in an IT infrastructure, testers use a wide variety of tools, techniques, and approaches. Penetration testing reveals the true worth of the threat and how it might damage the information system by going beyond just detecting vulnerabilities and guiding the tester through the process of exploitation, privilege escalation, and keeping up access to the system. A secure information system requires more than just vulnerability evaluation and penetration testing. Since most high-impact security breaches originate within an organization, clients and implementers of information systems should have some sort of control mechanism in place to prevent such breaches. This could also include measures to ensure that the information security of the business does not hinge on the availability of a single person. By supplying the necessary policies, tools, and processes for upgrading and sustaining a protected information system, Information Security Management Systems (ISMS) provide a comprehensive solution for a better information security experience.

When it comes to information security, the ISO/IEC 27001:2013 ISMS (Information Security Management System) is among the most stringent guidelines. The ISMS applies the necessary tools and techniques to ensure the confidentiality, integrity, and availability of the information system, covering almost every angle that might affect the security experience of the company. An information security policy must be developed as part of the ISMS in order to standardize the organization's systems and to recognize the obligations of its employees.

from the point of view of protecting sensitive data. The organization's internal communications are audited and updated in accordance with the information security policy on a regular basis. In this article, we have outlined the company's policy on the security of sensitive data. Policies should be drafted to ensure a consistent method of communication is in place inside the company for all of its functions. ISMS also applies a risk management method, which is an ongoing procedure of identifying the vulnerabilities mapped to their risk profile and of suggesting a mitigation approach [15], which goes above and beyond the vulnerabilities assessment and penetration testing.

LITERATURE REVIEW

Both physical and logical security were evaluated according to the methods used by Koldo Peca et al., namely ISO 31000 and ISO 27001. The only catch was that no security management was put in place to safeguard all possessions. [1]. Carol Hsu et al. evaluate the difference between companies with and without ISO 27001 certification in terms of productivity. Only financial data was unavailable for any of the companies [2]. ISO 27001 is a technique that should be implemented in an information security management, as explained by Manar Abu Talib et al. The plan for the future included assessing the new Information Security curriculum and developing better Information Security tools. [3]. The information was gathered via interviews and a review of the relevant literature by Elvi Fetrina and colleagues. The data gathered from this survey may be used for better stock control. Unified Modelling language was used for Rapid Application Development, which is an object-oriented approach. In this scenario, applying [4] raises concerns about the data's susceptibility to loss or harm. ISO 27001 is used by Awni Itradat and company to provide the highest level of security for their business. The only restriction is that the implementation team has to be well versed in the ISO 27001 Standard [5]. Reduced overall development costs and increased software quality and productivity are only two of the many benefits of Yogesh Verma and colleagues' web-based, centralized software asset management system. The lack of a regularly scheduled feedback system for continual development [6] was a significant shortcoming. Tabular presentation of the literature review.

TABLE 1
LITERATURE SURVEY

Sr.no	Author/Title &Publication	Technique/Algorithm	Limitations	Summary	Future Scope
1	Awni Itradat , Sari Sultan, Maram Al-Junaidi, Rawa’aQaffaf, Feda’a Mashal, and Fatima Daas, “Developing an ISO 27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study”, JJMIE, conference, April 2014	• ISO 27001 ISMS was used which guarantee an ultimate secure environment for organization.	• Should have all the knowledge ofISO 27001 Standard.	• Evaluated their • Define and prioritize their • Implemented ISO 27001 standard toel	• To reduce the cost of implement-ation
2.	Koldo Peciña, Ricardo Estremera, Alfonso Bilbao,Enrique Bilbao, “Physical and logical security	• Two methodologies are used ISO 31000 and ISO 27001 • Proposes a unique	• No security Management is implemented to	• Makes possible to comply with the all the compliances	• Need for a Centralized Security Manage

ISSN: 1832-5505

Applied GIS

Vol-7 Issue-02 April 2019

	management organization model based on ISO 31000 and ISO 27001”, IEEE, October 2011	procedure in which both, Physical and Logical Security are evaluated	ensure protection of all assets.		ment
Sr.no	**Author/Title &P**	**Technique/Algorithm**	**Limitations**	**Summary**	**Future Scope**
3.	Carol Hsu, Tawei Wang, Ang Lu, “The Impact of ISO 27001 Certification on Firm Performance”, IEEE, conference, January 2016	● List of firms with and without ISO 27001 certificates is collected ● Performance of each firm is compared	● Financial information isn	● The impact of ISO 27001 certification onfi	● Financial returns should be examined from ISO27 Certification
4.	Manar Abu Talib, Adel Khelifi, Tahsin Ugurlu,“Using ISO 27001 inTeaching Information Security”, IEEE, conference, October 2012	● ISO 27001 Standard procedures		● Importance ofin	● Evaluate theer improve theIn
5.	Martin Jakubicka, “Software asset management”, IEEE (International Conference on Software Maintenance), September 2010	● The main issues arising from several aspects such asleg ● It analyses the design of a software asset management system developedfor Univ this environment.	● No suitable methodology for creating SAM	● Creating SAMpr	● To increase the accuracy

6.	Elvi Fetrina, Eri Rustamaji, Tatat Nuraeni, Yusuf Durrachman "Inventory Management Information System Development at Bprtik Kemkominfo Jakarta", IEEE (5th International Conference on Cyber andIT Service Management (CITSM)), August 2017	• The data • Rapid Application Development (RAD) and Object-Oriented Approach using Unified Modeling Language (UML) were used asthe system development and design methods respectively.	• Possibility of loss or damage data	• Facilitate the performance ofas	• Could bee
7.	Afifah Muftinisa, Rosalina,Rikip Ginanjar, RB. Wahyu, Nur Hadisukmana "Development and Implementation of Fixed Asset Management System", IEEE (Second International Conference on Informatics and Computing (ICIC)), November 2017	• The system will help the company manage their assets, maintain a more detailed maintenance.	• Not muchfl	• Problem that was faced by the asset staff of the company has been successfully identified and analyzed	• Flexible asset depreciation is if to reduce a fixed asset's value

ISSN: 1832-5505

Vol-7 Issue-02 April 2019

Sr.no	Author/Title &P	Technique/Algorithm	Limitations	Summary	Future Scope
8.	Thomson Martin “An Introduction to Software Asset Management”, The ITAM Review/ Enterprise Opinions Limited White paper, January 2015	• There are a number of ways in which SAM can help an organization, but it takes a lot of time, effort and support from senior management.	• An expert with otherbu	• Every employee is ultimately a customer of SAM. asset needs to be managed correctly throughout its lifecycle	-
9	Yogesh Verma, R. Nandakumar, “Development of Software Asset Management System to Facilitate Software Reuse”, IET (Institution of Engineering and Technology) International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), December 2012	• This paper is to highlight the design and development of a web based centralized software asset management system. • System will aid in effective organizational software asset management and software reusability that will in turn improve thes productivity.	• No monitoringand evaluatingfor periodically using the built in feedback mechanism towards continuous improvement	• Facilitate software reusabilitythrough centralized archival	• To perform impact analysis of Asset Reuse and incorporating a credit system
10.	Viktor Shved, Pavel Kuzmich, Viktoria Korzhuk, “The Method ofan Audit of Software Containing in Digital Drives”, IEEE (8th International Conference on Application of	• Proposal of am operating systems and also with minor changes to the source code	• Implemented in the form ofprogram code in C++ • Advanced language inw	• Allows auditing the contents of digital drives to establish contained software • Can detect even the changed files,and files	• The method of executable file signature creating on the basis of behavioral patterns, thed

	Information and Communication Technologies (AICT)), October 2014				

RISK ASSESSMENT

A. *Introduction to Risk*

Apart from the health and security of our house we also have to take care of the risk which comes while running a business and its working environment. While considering the hazards in terms of business we have to consider all aspects from where the threat or intruder can affect our organization. To control all this hazards from affecting our organization certain action has to be taken to reduce or avoid and this action taken against the risk is called Risk Assessment.
Different control measures are applied to reduce the hazards from the organization depending on type of risk. There are many types of risks in an organization which can cause genuine loss of profits or even bankruptcy. To avoid these issue large

organization has a different department called Risk management which handles all the risk occurs in the organization but because of large investment small industries or organization can't afford to pay for it [15].

B. *Type of Risks*

Mainly there are five types of risks that organization faces:
1. Strategic Risk
The loss occurred in an organization by taking a poor business decision or implementing a wrong business plan. Everybody knows that for a successful business there need a comprehensive and a well business strategy plan. But sometimes the plan the organization takes is outdated or becomes less effective to reach desired objective. The strategic risk may include fail to achieve the desired objective, shifts in customer demands, strikes in the row material used by the organization or when a powerful new competitor enters in the market [16].

2. Compliance Risk
Consistence risk is also sometimes known as integrity risk. Many compliance regulations are enacted to guarantee that organizations operate decently and morally. Consistence risk is exposure to legitimate penalties, financial forfeiture organization faces when it fails to act as per industry laws and controls, internal strategies or prescribed best procedures.

Few examples of Compliance Risk

a. Workplace Health & Safety
The risk which deals with health and safety of the employee in the working environment such as stress accidents orstrain injuries

b. Corrupt Practices
Manly this risk is often done by the insiders such as employees which steal the confidential data of organizationfor bribery. Generally, organization is only responsible for these activates.

c. Environment Risk
The risks which can be harm for living organisms or the organization activities which can harm the environment.

d. Social Responsibility
This types of risk occurs when business activities harm their employee or the people of communities in which theemployees are working [17].

3. Operational Risk
Operational risk is the risk occurred due to wrong processes or procedures of an organization which causes change in value or objective of an organization. Following are the reasons which leads to operational risks:
a. System failures
b. Any event that disrupts business processes
c. Fraud or other criminal activity
d. Employee errors
Most associations acknowledge that their employee and procedures will naturally cause mistakes and add to errors in activities. In assessing operational hazard, practical remedial steps ought to be underlined so as to dispose of exposures and guarantee fruitful reactions. Poor operational hazard management can hurt an association's image and cause financial damage [16].

4. Financial Risk

Financial risk is the possibility that investors or other financial partners will lose money when they put their finance into an organization that has obligation if the organization's income demonstrates insufficient to meet its money related commitments. Many risk have a financial impact, in terms of additional expenses or lost revenue [16].

5. Reputational Risk

Reputational risk is a risk or threat to the name or position of a business or entity. Reputational risk can occur through various routes: directly as the result of the actions of the company itself; indirectly due to the actions of an employee or employees; or extraneously through other peripheral parties, for example, joint venture partners or suppliers. In addition to having good governance practices and transparency, organizations should be socially dependable and environmentally conscious to avoid or minimize reputational risk [16].

C. Identification of Risks

1.Identify the hazards- A standout amongst is the most essential parts of your Risk assessment which precisely identify the potential hazards in your working environment.

2.Evaluate the risks- Having identified the risk, we need to choose which risk can harm the organization the most from the likelihood and consequences factor which can rate from 1 to 5 or 1 to 100 depends on the organization but both likelihood and consequences can't be 0, it can be 0.1 but not 0. By observing both the factor we have to shield the organization to protect from the risk which has less likelihood and more consequence. Some practical steps you could take include [15]:

a. Attempting a less risky option
b. Preventing access to the risks
c. Organizing your work to reduce exposure to the hazard
d. Issuing protective equipment
e. Involving and consulting with workers

A global company starts its risk assessment process by considering the overall organization and divisional strategic objectives to guarantee that these objective are well considered and addressed to all through the risk assessment process. The risk assessment process includes

- Identifying risks at the divisional level considering both expected and unexpected or emerging risks.
- Assessing each risk for its likelihood, impact, and velocity (speed of onset and duration) on an inherent and residual risk basis.
- Considering both the inherent and residual risks by identifying the likelihood and impact without consideration of the control environment in place to mitigate the controls, then evaluating the adequacy of controls in place to mitigate the risk to determine the residual risk.
- Comparing and aggregating risks across the divisions and identifying synergies across the risks to ensure the highest level impact and probability is considered
- Using stress testing and scenario analysis to further consider the adequacy and completeness of risk assessments.
- Comparing residual risks to the company's risk appetite to identify gaps and the need for further actions andmitigations.
- Establishing risk categories for purposes of subsequent reporting and communication Reviewing risk assessment results with executive management and the board of directors for further considerations and oversight, particularly of identified actions to bring risks in line with the company's overall risk appetite.

D. Risk Mitigation

Risk Mitigation is the process to identify the risks and reduce the impact of risk faced by the organization. It is the way to reduces the impact of risk and loss on business Continuity. Risk mitigation helps to reduce threats that may put the organization in big loss including cyber-attacks, weather events and different reasons for physical or virtual damage. Although the principle of Risk mitigation is to set the business free of risk to increase the productivity of the organization. Risk mitigation focuses on some disasters and is used for those situation where a threat can't be avoided.

There are four types of Risk Mitigation

1. Risk Acceptance

Risk acceptance does not decrease any impacts anyway it is still considered a strategy management. This strategy is a common option when the expense of other risk the board choices for example avoidance or limitation may exceed the cost of the risk itself. An organization that wouldn't like to spend a lots of money on keeping away from risk that don't have a high possibility of occurring will use the method called as Risk Acceptance.

2. Risk Avoidance

Risk avoidance is the inverse of risk acceptance. The activity maintains a strategic that avoids every exposure to the risk.Note that Risk avoidance is typically the costliest of all risk mitigation options.

3. Risk Limitation

Risk Limitation is the most widely risk management strategy utilized by business. This strategy limits an organization's exposure by taking some action. It is a strategy employing an equal proportion or average of risk avoidance and risk acceptance. A case of risk limitation would be an organization accepting that a disk drive may fail and avoiding a long period of failure by having backups.

4. Risk Transference

Risk Transference is the involvement of transferring all the security and Risk assessment work to third party.

PROPOSED METHODOLOGY

Information Security Management System (ISMS) framework and the first stage of ISO/IEC 27001:2013 implementation will be discussed below. Organizational data security management is described by the ISMS management framework, which provides a systematic and effective approach. It defines the foundations of information security management and the processes by which it is implemented and kept up to date. Work begins at step 0 and continues through step 6 in Figure 1's ISO 27001 block diagram, which includes the Statement of Applicability and the Risk Treatment Plan. In these 6 phases, we'll address all of the activities specified in the ISO 27001 control Checklist. As may be seen in Figure 2, ISO 27001 has 114 controls.

The planning phase of implementing an ISMS entails developing and documenting the ISMS's policies, scope, risk assessment method, risk assessment plan, risk mitigation strategy, and Statement of Applicability (SOA), as well as implementing the ISMS's strategies and goals.

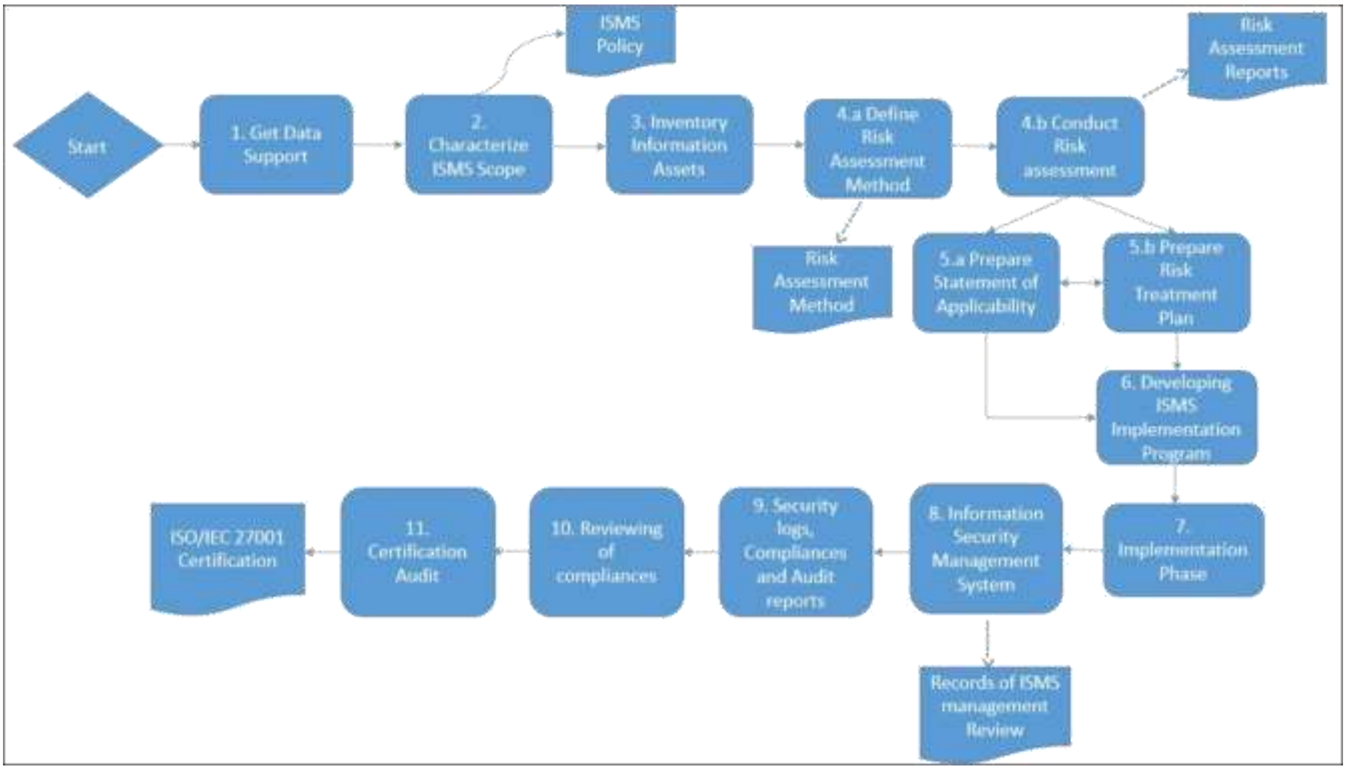
ISMS Policy
Risk Assessment Reports
Start
1. Get Data Support
2. Characterize ISMS Scope
3. Inventory Information Assets
4.a Define Risk Assessment Method
4.b Conduct Risk assessment
Risk Assessment Method
5.a Prepare Statement of Applicability
5.b Prepare Risk Treatment Plan
6. Developing ISMS Implementation Program
ISO/IEC 27001 Certification
11. Certification Audit
10. Reviewing of compliances
9. Security logs, Compliances and Audit reports
8. Information Security Management System
7. Implementation Phase
Records of ISMS management Review

Figure.1 Block Diagram of ISO 27001 [5].

The following are the required steps that you should follow for the implementation of ISO 27001.

Step 0. Start the Process

Start the process according to the ISO 27001 framework.

Step 1. Collecting the requirement of the organization

It is critical to distinguish and arrange objectives so as to increase full management support. To begin with, the essential objective of the organization can be extracted from however not limited to organization's main mission, IT objectives and other planned designs. Some important goals of the organization can be [14]:

a. Enhanced advertising potential

b. Affirmation and Authentication to other business partner of the organization's status in compliance with datasecurity.

c. Enhanced complete organization's income and benefits by giving most extreme security to customer's informationand data.

d. Support to organization's customers and partners about the organization's dedication towards data security,information and data insurance along with protection.

e. Appropriate consistence with industry guidelines and rules

Step 2. Get data Support

Involvement of Management is necessary for successful implementation of compliance with arranging, execution, continuous monitoring, operation, auditing and iterative improvement of security of organization. Steady dedication is must for consolidating activities, for example, ensuring that the right assets are open to the right employee to access to manage the ISMS of organization. It is essential to create support and excitement for the program from all levels of the corporation including upper management, mid-level management, and grass-root employees [14].

Step 3. Characterize ISMS Scope

According to the framework of ISO 27001 Standard, there are many scope which can be applied to the organization depending on the size of the organization. If you have a small organization, it is not necessary to apply all the controls present in the standard except the mandatory document which is mentioned. The control is selected according to the objective defined in the previous step. ISMS Scope must be specified in order to be get certified from external auditors [14].

Step 4. Writing a ISMS Policy

It is one of the mandatory document in the process of implementing. The policy should consist of basic issues and risk faced by the organization and information of framework used within your organization. The main focus of this policy is to explain your employees and resources what is the mission and vison of organization and how it can be achieved [14].

Step 5. Define risk assessment methodology

After getting the issues and risks faced by the organization that need to be reduced we have to formulate a proper risk assessment methodology. It should be followed in order to access, resolve and control the risk which is faced by the organization. We also have to identify and distinguish the resources from which the risk occurs and harm the organization security [14].

Step 6. Prepare Risk Treatment Plan

The process of Risk Treatment Plan includes distinguishing and categorize the risk as per their likelihood and consequences. Depending upon likelihood and consequences the risk should be treated accordingly. Every organization while implementing Risk treatment plan should follow the basic risk mitigation strategy which are accepting, avoiding, transferring, or reducing the risk to a certain level of acceptance. The plan also includes the total budget and what will do what, with whom. This is also an important step for implementing the project [14].

Step 7. 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. In this step a policy is prepared which will contain detailed procedures and statements of policy for the controls adopted by the organization along with a user responsibility.

Implementation program also includes awareness program to brief the employee about what it is and why this policy is important. If this awareness program is avoided, then it can be major reason for the failure of implementation of the project [14].

Step 8. Reviewing of compliances

After implementation phase, the organization should review all the compliances whether they are suitable for the objective of the organization to be achieved. Monitoring of objective, control, measurement methodologies comes together in this phase[14].

Step 9. Internal Audit

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

Step 10. Periodic Management Review

This department does not deal with the implementation of firewall for information security or implementing the policies and procedures of the project. 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].

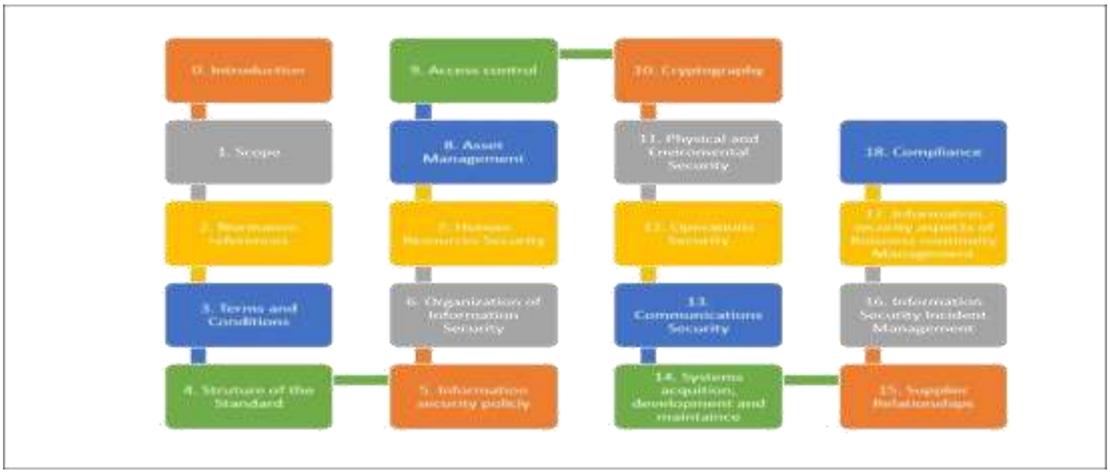
0. Introduction
1. Scope
2. Normative references
3. Terms and Conditions
4. Structure of the Standard
5. Information security policy
6. Organization of Information Security
7. Human Resources Security
8. Asset Management
9. Access control
10. Cryptography
11. Physical and Environmental Security
12. Operations Security
13. Communications Security
14. Systems acquition, development and maintaince
15. Supplier Relationships
16. Information Security Incident Management
17. Information security aspects of Business continuity Management
18. Compliance

Figure 2. ISO 27001 CONTROL.

There are 114 controls in ISO 27001 Standard. Some of the controls are mentioned below which are important for the implementation of Standard. These are as follows [18].

A.5 Information Security Policies

A.5.1 Management direction of information security

Objectives - To provide management direction and support to data security as per business prerequisites and relevant laws andcontrols.

A.5.1.1 Policies for Information Security - A set of policies for information security shall be characterized, approved by themanagement, published and communicated to employees and important to external parties.

A.5.1.2 Review of the policies for information security- The policies for data security will be reviewed at planned intervals or ifhuge significant changes occur to guarantee their continuing suitability, adequacy and effectiveness.

A.6 Organization of Information Security

A.6.1 Internal organization

Objectives - To establish a management system to start and control the implementation and operation of data security inside theorganization.

A.6.1.1 Information Security Roles and Responsibilities- All information security policies and controls are defined and allocated.

A.6.1.2 Segregation of duties- Conflicting duties and areas of responsibility will be isolated to reduce opportunities for unapproved or unintentional modification or misuse of the organization's assets.

A.7 Human resources Security

A.7.1 Prior to Employment

Objectives- To guarantee that employee and contract based employee understand their duties and are suit-able for the roles forwhich they are considered.

A.7.1.1 Screening - Background verification keeps an eye on all candidates for employment will be carried out in accordance with important laws, controls and morals and will be relative to the business requirement, the classification of the information to be accessed and the perceived risks.

A.7.2 During employment

Objective- To ensure that employees and contractors know about and fulfil their information security duties.

A.7.2.1 Management responsibilities -The Management will require all employees and contractual employees to apply data security as per the set up strategies and techniques of the organization.

A.7.2.2 Information security awareness,

education and training- All employees of the organization and, where significant, contractual employees shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as applicable for their job function.

A.8 Asset Management

A.8.1 Responsibility for assets

Objective- To identified assets which organization owned and defines the appropriate policies to protect it from threats.

A.8.1.1 Inventory of assets- Assets associated with data and information processing facilities will be recognized and aninventory of these assets will be drawn up and maintained.

A.8.1.2 Ownership of assets – Assets present in the inventory should be owned by the employee of an organization.

A.8.1.3 Acceptable use of Assets- Rules for the acceptable utilization of data and of assets associated with information andinformation preparing facilities will be recognized, recorded and executed.

A.9 Access Control

A.9.1 Business requirements of access control

Objective – To limit access to facilities and information from unauthorized users and parties.

A.9.1.1 Access control policy-A policy should be established, documented and executed for maintaining access control andprotecting unauthorized users to enter into the organization.

A.9.2 User access management

Objective- To ensure that authorized users access and to prevent unauthorized access in the organization.

A.10 Cryptography

A.10.1 Cryptographic controls

Objective- To ensure the confidentiality, integrity and authenticity of organization by encrypting the confidential data fromauthorized users.

A.11 Physical and Environmental security

A.11.1 Secure areas

Objective- To prevent unapproved physical access, damage to the organization's data and data processing facilities.

A.11.1.1 Physical security Perimeter-Security perimeters will be defined and used to protect areas that contain either sensitive orcritical data and data preparing facilities.

A.11.1.2 Physical entry controls -Secure areas will be ensured by appropriate entry controls to guarantee that only authorizedpersonnel have permit access.

A.11.2 Equipment

Objective- To prevent loss, damage, theft or compromise of assets and intrusion to the organization's activities.

A.14 System Acquisition, Development and Maintenance

A.14.1 Security requirements of information systems

Objective- To ensure that data security is an integral part of information systems over the entire life cycle. This additionallyincorporates the prerequisites for information system which give benefits over public networks.

I. RESULTS

According to ISO 27001 Standard till now we have implemented the Disaster Recovery Management in which regular backup of data has been taken to avoid the Data loss. Along with Disaster Recovery Management, we have taken out the report of all the installed and licensed system and application softwares of our Organization which lead to Human Resource management and Software Asset Management. The activities of employees and students is also being monitored which lead to access control and User Management.

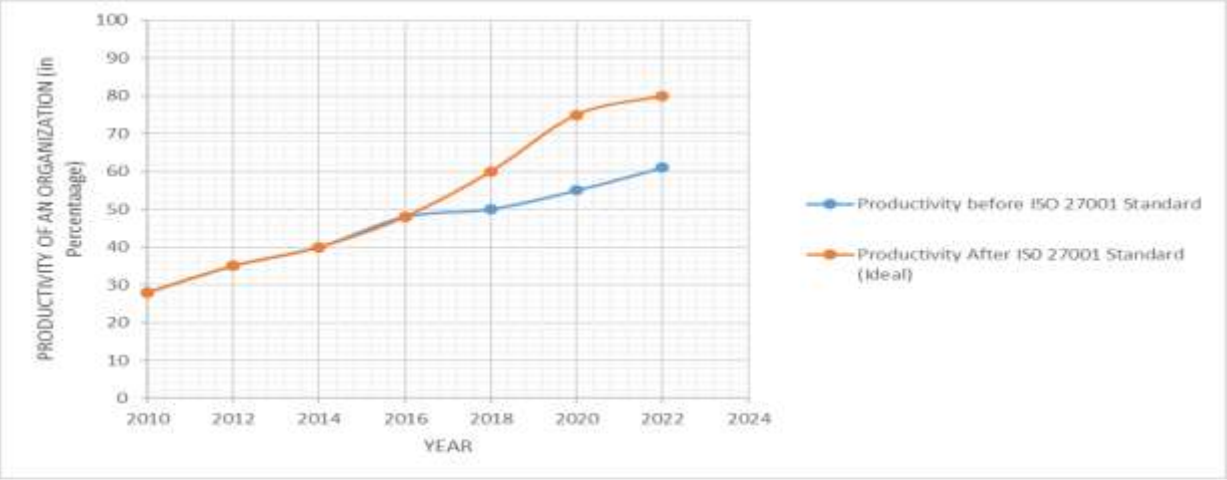

Figure 3. Ideal graph for ISO 27001 Standard.

Figure 3 shows the Ideal graph of an organization after implementing the ISO 27001 Standard. As the Standard gets into action, the productivity of an organization will increase simultaneously depending upon how it is being followed. The graph shows the productivity/ performance of the organization since 2010 to 2024 and shows how the productivity will affect positively after implementation of ISO 27001 Standard.

In figure 4 shows the Risk identified in an organization in last few years such as Data theft, Ransomware, Compliance risks, operational risks, Financial risks and Reputational Risks. As shown in figure 4 we have analysis the organization's risk since 2010 and predicating the reduction of percentage of risk in upcoming years

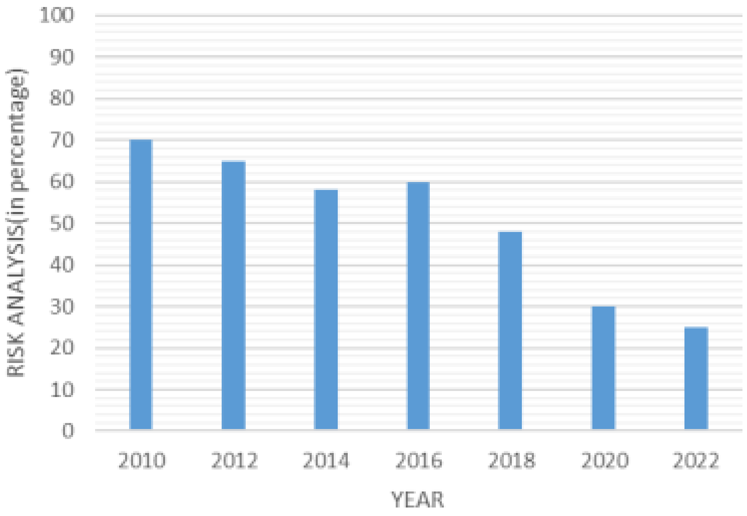

Figure 4. Risk analysis in past few years.

CONCLUSIONS

Organizations throughout the globe have recognized security breaches as a serious risk. Millions are spent annually by businesses and governments to repair the damage done by cyberattacks on their data. Numerous studies have shown that fixing an issue on the inside of a company is the most effective way to avoid security breaches. ISO 27001 Standard implementation might help businesses avoid all these problems. Consequently, many businesses are adopting information security management in order to equip themselves with the controls necessary to eradicate the internal organizational risks that may result in a devastating security breach.

REFERENCES

[1] Koldo Peciña, Ricardo Estremera, Alfonso Bilbao, Enrique Bilbao, "Physical and Logical Security Management Organization Model Based on ISO 31000 and ISO 27001", IEEE Carnahan Conference on Security Technology, 18-21October 2011

[2] Carol Hsu, Tawei Wang, Ang Lu, “The Impact of ISO 27001 Certification on Firm Performance”, IEEE, 2016 49th Hawaii International Conference on System Sciences (HICSS), 5-8 January 2016

[3] Manar Abu Talib, Adel Khelifi, Tahsin Ugurlu, “Using ISO 27001 in Teaching Information Security”, IEEE, IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society, 25- 28 October 2012

[4] Elvi Fetrina, Eri Rustamaji, Tatat Nuraeni , Yusuf Durrachman, “Inventory Management Information System Development at Bprtik KemkominfoJakarta”, IEEE 5th International Conference on Cyber and IT Service Management (CITSM), 8-10 August 2017

[5] Awni Itradat, Sari Sultan, Maram Al-Junaidi, Rawa’a Qaffaf, Feda’a Mashal, and Fatima Daas, “Developing an ISO 27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study”, JJMIE (Jordan Journal of Mechanical and Industrial Engineering) ISSN 1995-6665 Volume 8, April. 2014

[6] Yogesh Verma, R. Nandakumar, “Development of Software Asset Management System to Facilitate Software Reuse”, IET (Institution of Engineering and Technology) International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), 19-21 December 2012

[7] Afifah Muftinisa, Rosalina, Rikip Ginanjar, RB. Wahyu, Nur Hadisukmana “Development and Implementation of Fixed Asset Management System”, IEEE
(Second International Conference on Informatics and Computing (ICIC)), 1-3 November 2017

[8] Viktor Shved, Pavel Kuzmich, Viktoria Korzhuk , “The Method of an Audit of Software Containing in Digital Drives”, IEEE he Method of an Audit ofSoftware Containing in Digital Drives, 15-17 October 2014

[9] Paul Hopkin, “Fundamentals of Risk Management Understanding, evaluating and implementing effective risk management”, Kogan Page, July 2018

[10] Tsan-Ming Choi, Hing Kai Chan, Xiaohang Yue, “Recent development in Big Data Analytics for Business Operations and Risk Management”, IEEETransactions on Cybernetics, 12-16 January 2017

[11] Benno E. Albert, Rodrigo P. dos Santos, Cláudia M. L. Werner, “Software Ecosystems Governance to Enable IT Architecture Based on Software Asset Management”, IEEE 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST), 24-26 July 2013

[12] ISO/IEC/IEEE 26531, International Standard, “System and Software Engineering – Content management for product life –cycle, user and servicemanagement documentation”, May 2015

[13] ISO/IEC19770-1, “International Standard, Informational Technology – IT asset management”, December 2017

[14] SYNC RESOURCE (2018) ISO 27001 (ISMS) Metrics And Step By Step Implementation Guide 2018. [Online].Available: https://blog.sync- resource.com/2018/04/19/iso-27001-implementation-step-by-step-guide/

[15] NEWS WEB ZONE (2017) A Brief Guide to Controlling Risks In The Workplace [Online]. Available: https://www.newswebzone.com/brief-guide- controlling-risks-workplace/

[16] Envato tuts+ [2014] The Main Types of Business Risk [Online]. Available : https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693

[17] Simplicable [2016] 6 Types of Compliance Risks [Online]. Available : https://simplicable.com/new/compliance-risk.

[18] THYCOTIC | ISO 27001[Online]. Available : http://www.esdebe.com/perch/resources/iso-27001-annex-s-control-mapping.pdf