Maryanne Ndungu and Sushila Kandel

INFORMATION SECURITY MANAGEMENT IN ORGANIZATIONS

Thesis

CENTRIA UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information Technology

June, 2015

Unit	Date	Authors
Kokkola - Pietersaari	June 2015	Sushila Kandel and Maryanne Ndungu
Degree programme Information Technology		
Name of thesis INFORMATION SECURITY MANAGEMENT IN ORGANIZATIONS		
Instructor Nina Hynynen		**Pages** [43]
Supervisor Dr Grzegorz Szewczyk		

In today's globally interconnected economy, information security has become one of the most complex issues of concern at the world's leading organizations. The capital value of information is significantly increasing and forming a large part of the shareholder value due to increased dependence on information. Organizations that want to achieve competitive advantage amongst other goals have information security at the centre of their concerns.

It is now evident that information is a business enabler and it is almost impossible for an enterprise in today's information economy to transact its business with ineffective information security. Inadequately protected organizations have turned out to be threats for their more secured counterparts. Information security is not an option for organizations that wish to maintain uninterrupted business processes.

The aim of this thesis work was to illustrate the importance of information security and its value. This thesis recognizes that information security is not only a technical issue but a governance concern as well. IT security governance structure and its importance are therefore emphasized. This thesis discusses the procedures to be followed by organizations to ensure their information is secure. It includes an in depth focus on the establishment of an organization's unique security policy document.

Key words
Information security, information security management system, technology, security governance.

Concept Definitions

CIA – Confidentiality Integrity Availability

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CISSP – Certified Information System Security Professional

COBIT – Control Objectives for Information and Related Technology

ePHI – Electronic Protected Health Information

IEC – International Electrotechnical Commission

ISACA – Information Systems Audit and Control Association

ISMS – Information Security Management System

ISO – International Organization for Standardization

IT – Information Technology

ITGI – Information Technology Governance Institute

ITIL – Information Technology Infrastructure Library

NIST – National Institute of Standards and Technology

SP – Special Publication

SSL VPN – Secure Sockets Layer Virtual Private Network

TABLE OF CONTENTS

ABSRACT

CONCEPT DEFINITIONS

1 INTRODUCTION 1

2 VALUE OF INFORMATION 3

3 INFORMATION SECURITY GOVERNANCE 7

3.1 Top Management(Board of Directors) 8

3.2 Security Project Managers 9

4 RISK MANAGEMENT 11

4.1 Risk Analysis 11

4.2 Risk Assessment 12
4.2.1 System Characterization 14
4.2.2 Threat Identification 14
4.2.3 Vulnerabilities Identification 14
4.2.4 Control Analysis 15
4.2.5 Likelihood Determination 15
4.2.6 Impact Analysis 15
4.2.7 Risk Determination 16
4.2.8 Control Recommendations 16
4.2.9 Result documentation 16

4.3 Risk Reduction 17

4.4 Evaluation and Assessment 20

5 INFORMATION SECURITY POLICIES 21

5.1 Importance of security Policy 21

5.2 Information Security Frameworks and Tools 22
5.2.1 ISO 27000 22
5.2.2 NIST 24
5.2.3 ITIL 24
5.2.4 COBIT 25

6 INFORMATION PROTECTION 26

6.1 Physical Protection 26
6.1.1 Cabling 26

6.1.2 Protective rooms for devices 27
6.1.3 Access control 27

6.2 Administrative works 28
6.2.1 Training 28
6.2.2 Secure Business Rules 29
6.2.3 Access control to Networks 29
6.2.4 User's authentication 30
6.2.5 Decentralization of Administration 30

6.3 Data and Networks protection 30
6.3.1 Backups 30
6.3.2 Secure Remote access 31
6.3.3 Secrecy of Information 31
6.3.4 Firewall 32
6.3.5 Anti-virus protection 32
6.3.6 Inspection of communication 32
6.3.7 Intrusion observation 33

7 DAY TO DAY ACTIVITIES 34

7.1 Information System's Inventory 34

7.2 Human Resources Security 35

7.3 Information security Culture 35

8 OBSERVATION OF CHANGES AND MAINTENANCE 37

9 CONCLUSION 40

REFERENCES 41

1 INTRODUCTION

The world has become a global village thanks to the widespread use of the internet where with a click of a mouse, a single idea can reach billions of people across the globe. The benefits of information for organizations are undeniably vast. Information is currently the driving force of businesses and economies due to the globalization of products and markets. The internet has enabled information availability therefore making it a most valuable information source and a means of information transmission. The barrier brought about by location is beginning to subside as virtual businesses are currently running round the clock. Increased dependency on information by organizations has consequently led to an increase on the dependence of the CIA (Confidentiality, Integrity and Availability) paradigm of information.

Global connectivity and availability of information although positively impacting the world, also pose as real danger. The interconnected world offers an opportunity for people to perform actions that would result in life transforming solutions. On the other hand, individual actions have the potential to cause grievous damage. The development and speedy growth of the information economy has given rise to information security urgency. Additionally, organizations are facing advanced global risks and vulnerabilities. Newsrooms and publication houses have records of stories about immense losses experienced by organizations due data breaches or loss of information. It is a common belief among most executives and managers that their organizations are utterly safe. The harsh reality is that every organization will be attacked but the question is when and how severely.

Complexity and sophistication are some of the words that describe information security today. Information security's main aim is to protect the confidentiality, integrity and ensure availability of information infrastructure. It is concerned with guarding information from involuntary or deliberate misuse. The need for sound governance and management of information security is taking on a new urgency. The main objective of this thesis is to

explore the governance strategies and procedures to be considered by executive directors and managers while establishing globally recognized information security best practices. Although this paper deals with a technology issue, it is more concerned about governance rather than technical issues surrounding information security. It is therefore a suitable reference for board of directors, shareholders, executives and managers responsible for the leadership of information dependent organizations.

In an ISMS (Information System Management System) structure top management consists of the board of directors, executives and shareholders. The desired state of security in an organization can only be reached if top management is fully committed to oversee its development. Risk analysis and risk management are important for the purpose of identifying speculative risks, eliminating them or minimizing them to acceptable levels. An organization's policies outline the correct procedures that should be taken in certain circumstances. This thesis further outlines different measures that should be taken to ensure physical and network security. Day to day activities and maintenance should be observed and after reasonable amount of time they determine whether a new risk analysis is needed.

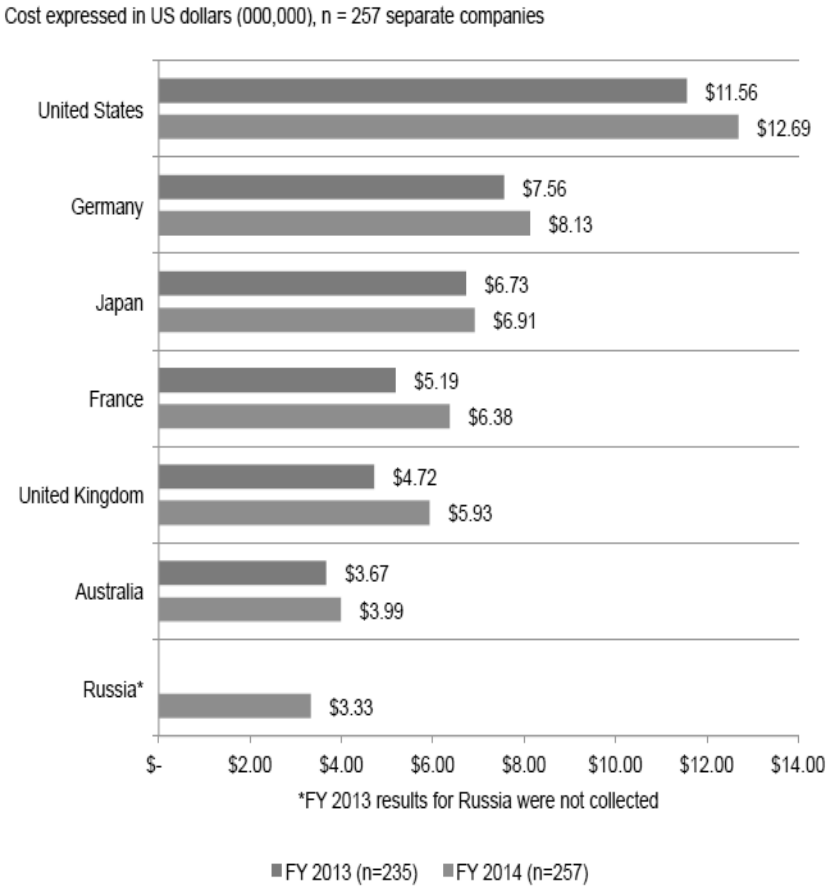
2 VALUE OF INFORMATION

Both organizations and individuals have sensitive information that requires adequate protection. Organizations will certainly be in possession of delicate information on their staff, budget, financial reports and business strategies. For the purpose of gaining competitive advantage, organizations will have research reports, trade secrets and other forms of sensitive data. Today, information is viewed as the lifeblood of the present-day enterprise. The dependence on information by organization is rapidly increasing and for some organizations, its loss implies loss of business. Individuals perform various tasks on their computers such as online shopping, e-banking and visiting social networks. Their computers therefore contain critical personal information that needs to be secured. (Mindful.com 2009.)

Information or security breaches take place when information is not sufficiently secured and unauthorized persons are able to access it. An information breach can lead to serious consequences. For organizations, a breach normally involves serious financial losses, costly law suits, reputational damage and in extreme cases loss of business. Identity theft, financial loss and damage to one's credit rating are some of the consequences of an information breach for individuals. Information breach recovery takes many years and the financial damages are harsh. (Ponemon Institute 2014.)

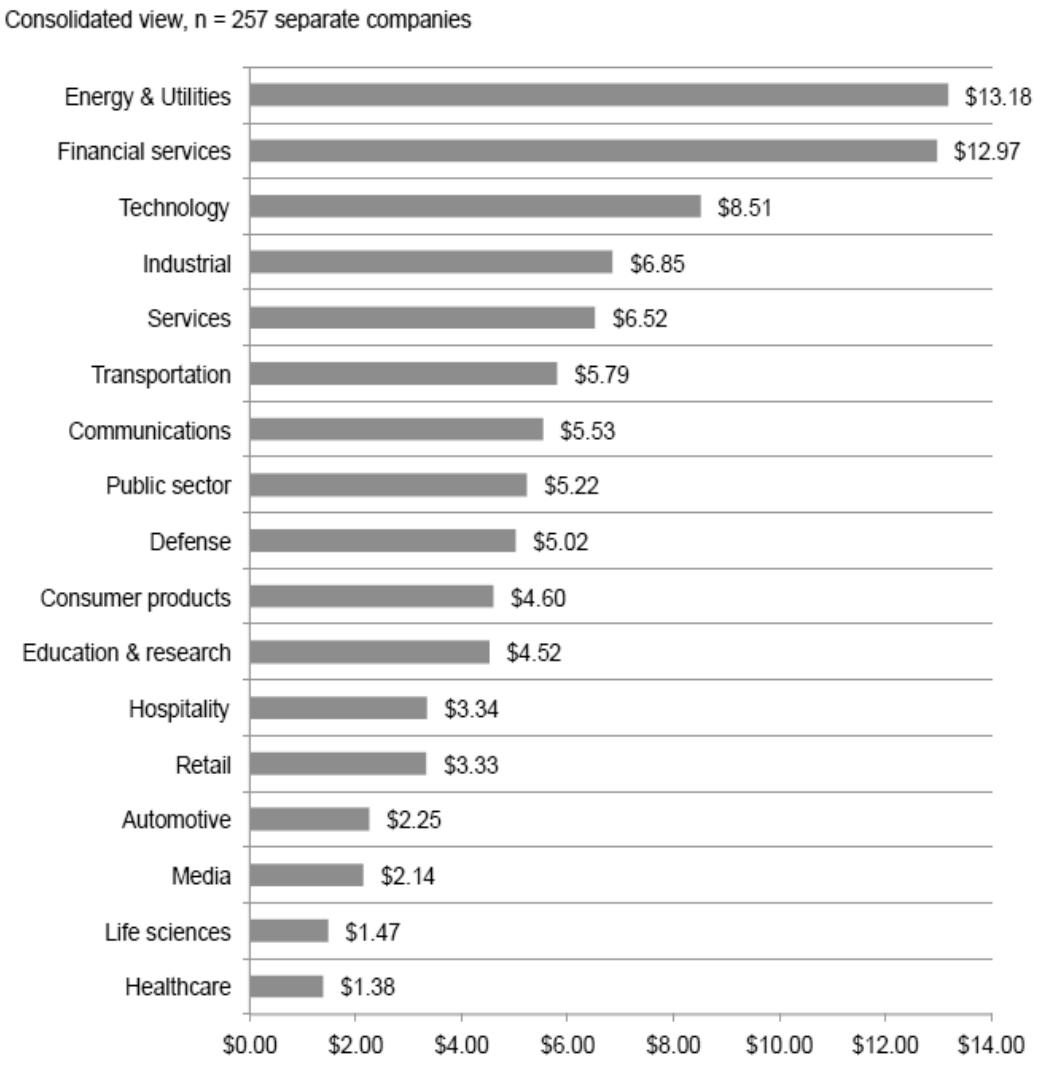
Breaches and data loss incidents are now becoming unavoidable phenomena for organizations of all types and sizes. While large and diverse amounts of data are being accumulated on various storage devices and service providers, businesses should be on high alert for imminent loss. Business came to a standstill at Target in 2013 when an information breach occurred. An estimated 110 million credit and debit card records were exposed as a result. This incident brought to light the intensity of damages caused by a breach ranging from paralysis of business activities to immense financial losses not forgetting consumer remorse. The compromised credit and debit cards belonged to several banks which therefore became victims of the incident, too. (Online Trust Alliance 2014.)

In 2014, the Ponemon institute conducted a study on cyber crime with the purpose of quantifying the economic impact of cyber attacks. This study was conducted in the United States, United Kingdom, Germany, Australia, Japan, France and Russia. The results of the study have determined that the highest total cost of data breach is $12.7 million and the lowest was found to be $3.3 million. The study involved 257 organizations and the average annual cost was found to be $7.6 million which is a 10.4 percent increase from the previous year, 2013. It is also evident that cyber crime is on the rise with all the six countries experiencing a net increase in the cost incurred as a result of cyber crime compared to the previous year. The United Kingdom, for example, experienced an increase from 2.7 percent in 2013 to 22.7 percent in 2014. Graph 1 below shows the comparison between 2013 and 2014 total cost of cyber crime for the seven countries as was found by the Ponemon institute. (Ponemon Institute 2014.)

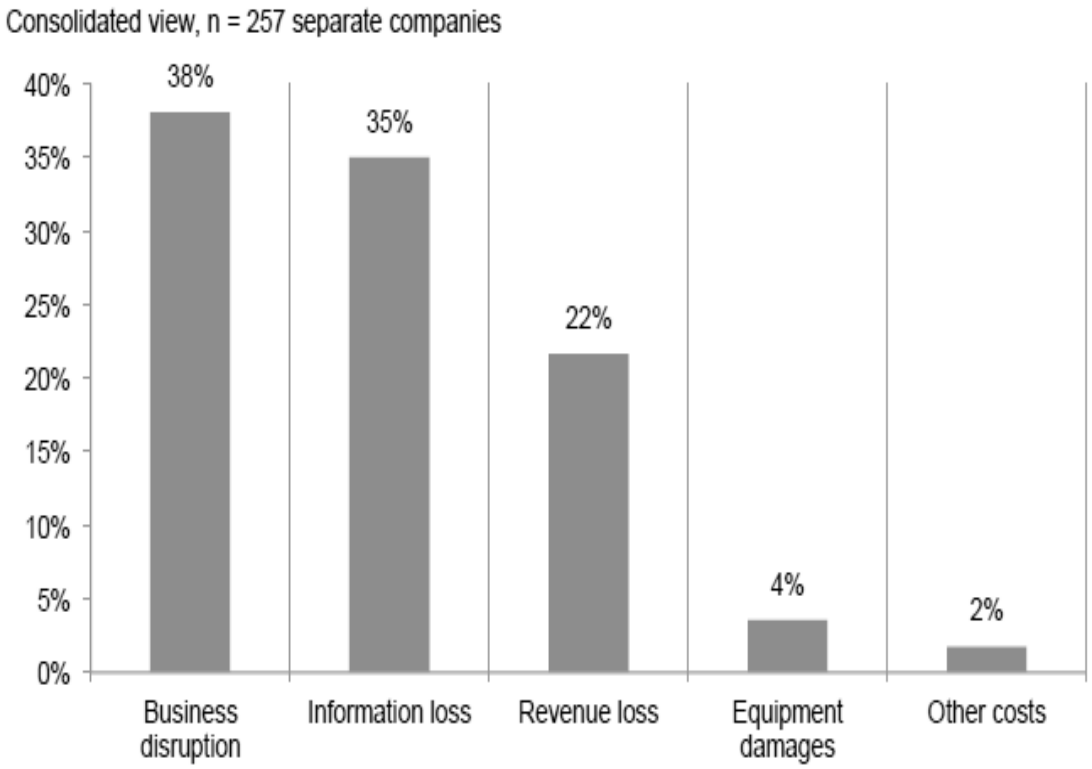


Graph 1: Total Cost of cybercrime (Ponemon Institute, 2014).

There is a major misconception that information security is a concern only when the organization is holding very important trade secrets or when that organization is Coca Cola with the secret formula for Coke. Although at different levels, cyber crime poses a threat to all industries. Ponemon institute compared in their study, the average cost of cyber crime in different industries and the results are as shown in Graph 2 below. Energy and utilities and the financial sectors appear to bear the most implications should a security breach occur. (Burgess & Power 2008.)



Graph 2: Average Cost by industry (Ponemon Institute 2014).



Graph 3: Percentage cost for consequences (Ponemon Institute 2014).

According to Ponemon institute, the primary consequences of cyber crime involve business disruption, loss of information, loss of revenue and damage of equipment. The graph 3 above shows business disruption as the most expensive consequence of an information breach at 38 percent. Business disruption includes reduced productivity and a pause in business processes. Loss of information and loss of revenue follow at 35 percent and 22 percent respectively. (Ponemon Institute 2014.)

3 INFORMATION SECURITY GOVERNANCE

Secure flow of information plays a vital role in today's economy and should therefore be treated with due importance. More often than not, Information Security is single-handedly dealt with as a technology issue rather than treating it as a governance issue as well. According to the IT Governance Institute (ITGI), governance is a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (CISSP Guide to Security Essentials 2010). Although it is the responsibility of the executive management to deal with the technical aspects of information security, the board of directors are expected to include the information security concern in the organization's governance undertakings. The role of integrating information security into the governance framework is the responsibility of the board of directors, who, despite acknowledging the need to uphold the integrity and continuity of business processes, regrettably have superficial knowledge of information security. (IT Security Governance - CIO, CISO and Practioner Guide 2009.)

> Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance (Greene 2014)

3.1 Top Management(Board of Directors)

The Board of Directors is a body with the authority to make the policies of an organization and has an obligation to superintend the development and maintenance of the information security management system project. The term “superintend” is used to describe the supervisory function of the board of directors. The management is therefore left with the responsibility of day-to-day management. While developing the security system, it is the duty of the board to ensure that the policies are aligned with the organization’s objectives. For conventional development, organization and maintenance of the security program, support and resources are required and this ought to be provided by the executive management. (Greene 2014.)

The status of information security in organization highly depends on the appropriateness of the security policy. The effectiveness of the security policy is in turn dependent on the board’s level of understanding of information security. The objectives of an organization are the determining factor of the organization’s information requirements and therefore the need and importance of information security. An important question for the board of directors at this point is whether the board understands the criticality of information security to business processes and business continuity. Until the board has sufficient knowledge of the criticality of information security, inadequate support for security systems may be allocated resulting in defective risk mitigation activities. More often than not, board directors only realize the extent of information security risks after a grievous incident occurs with severe consequences. (Kajava, Antilla, Varonen, Savola & Roning 2006.)

Acknowledging the importance of information security is succeeded by positioning information security on the board’s agenda. Considering the value of information to an organization, it is crucial to integrate information security ventures into the governance framework. This requires that the board is on the fore-front in the development of an information security system and suitable programs. The board’s commitment is demonstrated by its support towards the development and implementation of sound

information security policies and a framework that meets international standards. All users of the information system ought to know their duties and responsibilities in ensuring confidentiality, availability and integrity of information. This is conveyed by means of a documented statement. The policy statement should be assimilated into the overall governance program for the purpose of routine review, monitoring and maintenance. (Greene 2014.)

A telling question into the development of information security program is whether sufficient resources are allocated to establish an appropriate security framework. The essential component of efforts towards securing information is evident support and involvement of top management. Essentially, this commitment includes allotting significant portion of funding to information security work and proactively responding to new incidents. The enterprise's information security management requires committed leaders to be effective in the long-term. Members of the board should therefore identify information security leaders who will take the responsibility of managing the information security system. The leaders have to keep the members of the board updated on the status of information system. Clear roles and responsibilities should be illustrated in order to establish accountability. (Tung 2014.)

3.2 Security Project Managers

Information security project managers have the responsibility of overseeing the implementation of new security drives or upgrades to current systems. It is the interest of managers that information is shared only with authorized persons. Their responsibility is to ensure that the information is verifiably authentic, complete, sufficiently accurate, trustworthy and reliable as well as accessible when needed. Special attention is paid to maintaining the CIA paradigm of information security during the development of security systems. (SANS 2013.)

The development of an information security management system is a highly iterative process and therefore security considerations in each stage are vital. The most convenient opportunity to establish security practices is during the early phases of the process during initiating and planning. In the initiating phase, the manager must check that the project makes a significant change in the security status of the organization and offers protection in any circumstance. The benefits of implementing the project should be worth its costs. The planning stage involves consideration of schedule, scope and cost. A revealing question into these aspects is whether the project's deliverables are highly demanding and may materially influence the schedule and cost. (SANS 2013.)

The safety, security and availability of communication channels should be considered vital in the executing stage of development. Communications need to be secured via meeting pass codes and all devices securely configured with passwords and encryption. Documents need to be safely stored and backed up at appropriate time intervals. The monitoring and controlling stage requires that risks and mitigations be regularly reviewed with the board of directors and stakeholders. The deliverables of the project are to be verified to check whether they meet the security requirements. (SANS 2013.)

4 RISK MANAGEMENT

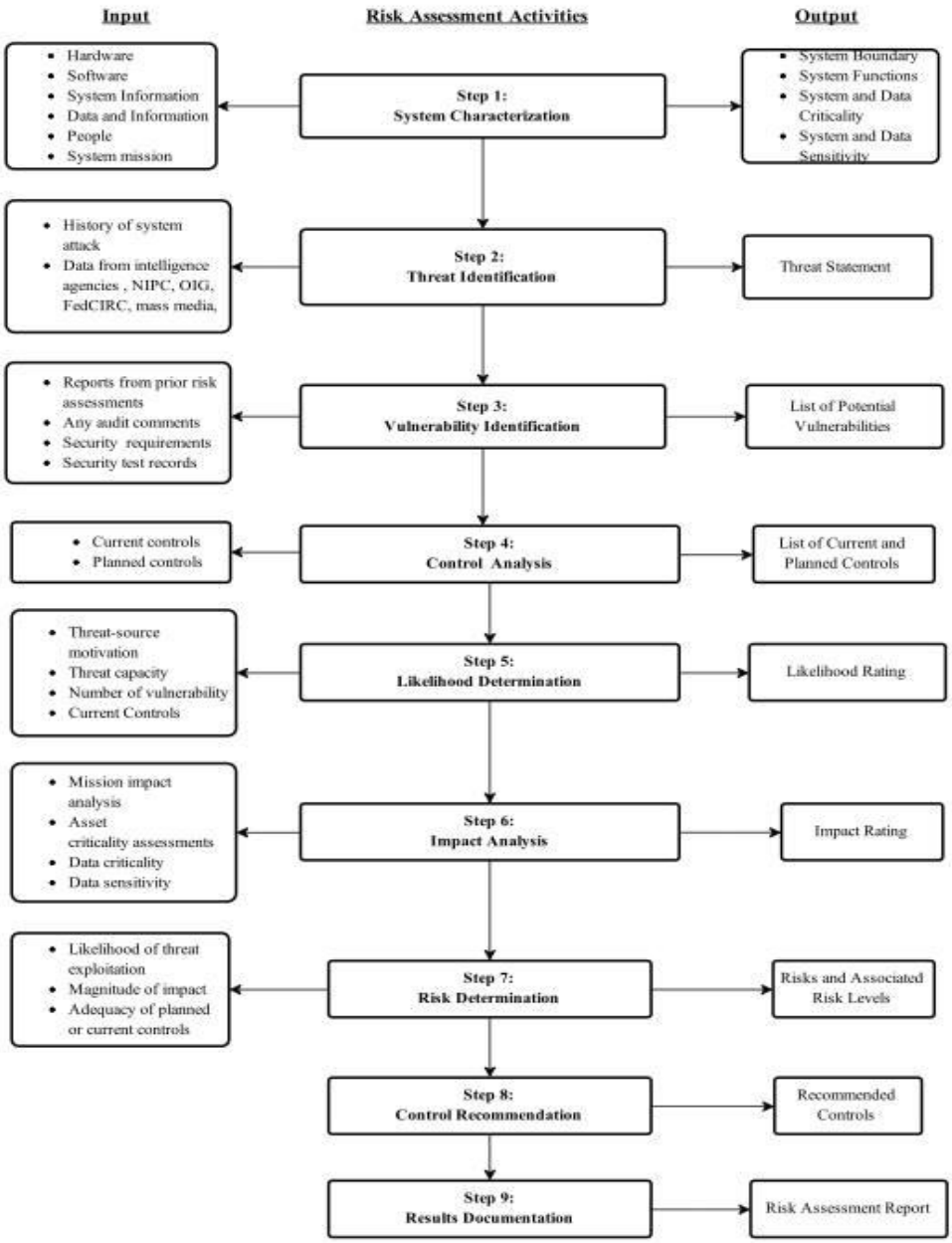
Risk management is a process that accord organization to balance their operational and financial cost of safeguarding measures and achieve their mission goal. It is not bounded by the information technology and security rule. It is a process which helps enterprises to meet their goals and protect organization´s assets. It helps to identify, control and reduce the impact of vulnerabilities. The main goal of this process is to minimize the risk while performing few activity or function which can be approved by the senior management. The ubiquitous nature of communication and information technologies means that the risks can become a complicated mesh of unmanageable interdependencies. There are mainly four processes in the risk management which are risk analysis, risk assessment, risk reduction as well as evaluation and assessment. (Peltier 2005; Humphreys 2010.)

4.1 Risk Analysis

Risk analysis is a technique used to identify and assess uncertainties that may have severe impact on the assets of the organizations. This process is also called impact analysis. This process helps to identify the most important source of uncertainty and evaluate its magnitude. It requires a cost benefit analysis where the features and benefits of the asset are reviewed. These costs include the information about the development and maintenance of the process that are held in the organization e.g. documentation development, user and infrastructure support training and possible upgrades. Another important factor to take risk analysis into account is the impact of regulatory compliance issue. Every new project should be examined under regulatory requirement to avoid risk. For risk analysis and risk assessment, the need to determine due alertness is an important factor. The main reason to conduct this process is that it makes good business sense. Thus, every organization should follow this process based on their need and ability in order to achieve their business goal. (Peltier 2005.)

4.2 Risk Assessment

Risk assessment is the process where you identify the hazards and try to evaluate them. It is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard). Organizations use risk assessment to determine the range of the potential threat and the risk associated with an IT system. The result of this process helps to identify the essential control measures. Risk is a function of the likelihood of a given threats-sources performing a particular potential vulnerability. Therefore it is important to find the possible threats to an IT system where risk must be analyzed under supervision with the potential vulnerabilities and the controls operating for the IT system. An impact refers to the magnitude of harm that could be caused by a threats exercise of vulnerability. The level of impacts is governed by the potential mission impacts and in turn produces a relative value for IT system components. (Humphreys 2010.)



Graph 4: Risk assessment methodology flowchart (Gary Stoneburner 2002).

Graph 4 shows the risk assessment methodology flowchart. This flowchart provides information about the inputs and outputs in risk assessment activities. It consists of nine different steps concerning various areas in risk assessment.

4.2.1 System Characterization

In assessing risk for an IT system, the first task is to define the process, application, system, or assets in order to find the possible effort. The limitations of IT systems are then analyzed, along with the resources and the information that are found in the system. This helps you find the essential information which defines the possible risk. (Peltier 2010.)

4.2.2 Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. The purpose of this step is to identify the possible source of threat and compose them into a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. The common threats can be natural, human, or environmental. In order to identify the threat source, it is really important to consider all potent threat sources that could bring complication. (Peltier 2010.)

4.2.3 Vulnerabilities Identification

Vulnerability is the flaw or weakness in the system security process, design, implementation, or internal controls that could be applied and result in a security breach or a violation of the systems security policy. The vulnerabilities may be identified in different areas in an organization e.g. process and procedures, management routine, personnel, physical environment, hardware, software and dependencies in external parties. These vulnerabilities do not cause harm in itself as long as there is a threat to exploit it. But they should be minimized by using effective control to avoid any loss of information.

4.2.4 Control Analysis

The main aim of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to reduce or eliminate the possibility of a threat applied in the system. The organizations should implement cost effective controls which helps them to determine the impact of implementing a new control. It avoids the unnecessary work or cost i.e. the duplication of controls. While identifying the existing controls, it is important to ensure that if the control measure is working correctly or not – a reference to existing report from ISMS helps to reduce the loss of time and money. If the control does not work it creates likelihood in IT system. Thus analyzing the effect of the controls helps to reduce the possible threats in the future. (Peltier 2010.)

4.2.5 Likelihood Determination

These determine the rate of probability that a potential vulnerability may in practice within the associated environment. It depends on the different factors like threat-source motivation, a nature of motivation and the effectiveness of control measures. It helps to know the consequences to the assets and business processes. It is important to assess the likelihood of each case and the impact that it causes using qualitative and quantitative estimation techniques. The possible vulnerability can be distinguished in three phases namely high, medium, or low. (Peltier 2010.)

4.2.6 Impact Analysis

In this step the level of risk is to determine the adverse effects from a successful threat practice. It is necessary to have detail information about the systems mission, criticality and data sensitivity. These all information can be gained from the documentation done by the organization. Therefore; the adverse impact of a security event can be described in

terms of loss or degradation of any, or a combination of any, of the following three security goals of integrity, availability, and confidentiality. (Stoneburner 2002.)

4.2.7 Risk Determination

The main aim of this step is to assess level of the risk of the IT system in the organization. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of possibility of a given threat-source, magnitude of impact and adequately planned security controls. It is based on assessed consequences and likelihood. In addition, appropriate risk evaluation can be considered as economically effective that concerns stakeholders and other variables. (Stoneburner 2002.)

4.2.8 Control Recommendations

The main purpose of this process is to control the identified risk. The recommended controls are to mitigate the level of risk of the IT system and maintain the data to an acceptable level. There are few factors which should be taken into account when recommending controls in order to minimize risks. They are: effectives of recommended options, legislation and regulation, organization policy, operation impact, safety and reliability. (Stoneburner 2002.)

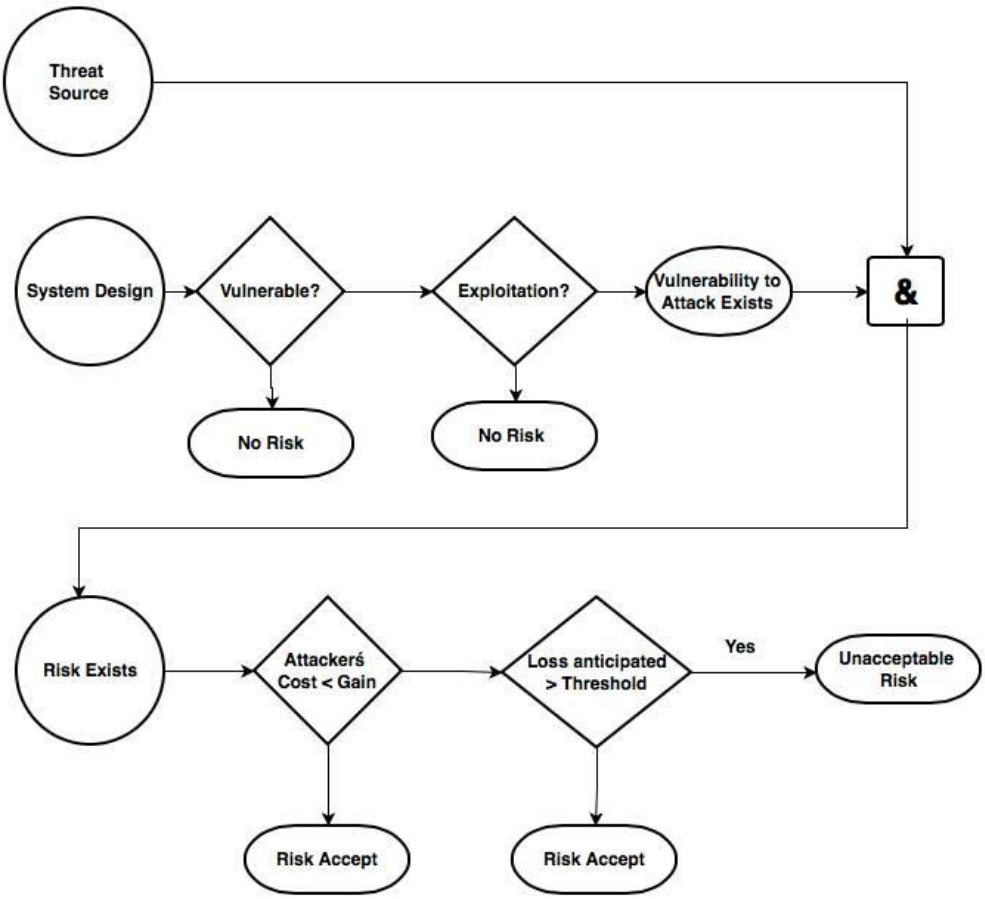
4.2.9 Result documentation

The final process of the risk assessment should be made in an official report. It helps the senior management, the mission owners, and decision makers on policy, budgeting and

system operational management changes. The documentation should be made in a systematic manner and analytical approach to assess the risk which helps management to understand the risk and make resources available where needed. This is the reason why most of the personnel prefer to address the threat pairs as observations instead of findings in the risk assessment report. (Peltier 2010.)

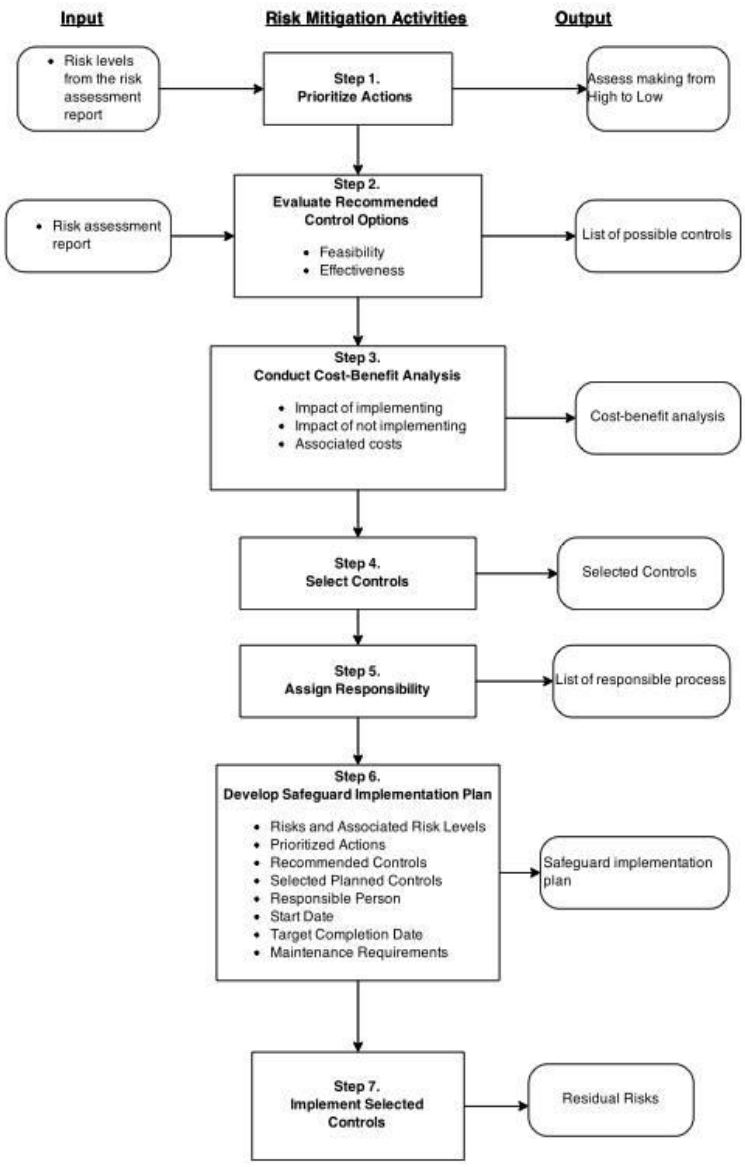
4.3 Risk Reduction

Risk reduction is the second process of risk management which involves compiling, evaluating and implementing the appropriate risk-reducing controls recommended from the risk assessment process. It is almost impossible to eliminate all risks, therefore is the responsibility of the functional management and business managers to use a economic approach and implement the most relevant controls to decrease risk to an acceptable level, with minimized conflicting impact on the organization resources and mission. There is a systematic method used in risk management in order to reduce mission risk for example by assuming the risk, avoiding the risk by using control measures and appropriate planning of implementation of controls. Every organization has a different risk reduction strategy. The management knows the potential risks and recommends the control measures when and under what condition action should be taken. Also it gives information about when to implement control measures. (Stoneburner 2002.)



Graph 5 Risk reduction action point. (Stoneburner 2002).

Graph 5 above provides the information useful in a case where the vulnerability exists there should be implementation of assurance technique to reduce likelihood of threats. When the flaw can be recognized then the protection layer and administrative controls should be applied to minimize the risk. When the cost of attacker seems to be less than the potential gain, much power protection layer should be implemented to discourage the attackers motivation by increasing its cost. When the loss is too great for the security system then apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attacker. (Stoneburner 2002.)



Graph 6: Risk reduction methodology flowchart (Stoneburner 2002).

The graph 6 presented above shows the implementation of control measures. The implementation actions are arranged from top priority to low priority. These assist to protect the organization from risk. Not all the risk assessment process is relevant and feasible with all the organization. The main aim is to select most useful control measure to minimize risk. In order help management in decision making and to identify the economic approach. In step 4 assigning responsibilities to the most skillful and expertise personnel will help to reduce organization risk. Implementing all this control measure does not eliminate the risk but it saves the organization from hazards. (Stoneburner 2002.)

4.4 Evaluation and Assessment

The network is expanding and updating day-by-day. The IT system which most organizations use get changed or updated with the newer versions. In this situation the previous risk reduction strategy might not work efficiently. This raises more concern in the risk management process. The risk can be reduced by following a good security practice. Risk management should be held and integrated in the SDLC for the IT systems, not because it is a requirement by law but it is a good practice to support the organization's mission. The management should make a specific schedule for assessing and reducing risks. Also the assessing process should be flexible enough that allows the changes where needed, such as major changes in IT system and processing environment due to the changes in the technologies and policies. The key of successful risk management depends on the commitment; full support and participation from the IT team, capability of risk assessment team which has expertise experience in applying good risk assessment methodology. The awareness among the personnel working in the organization concerning implementation of the control measures in case of any vulnerability helps to maintain the missions of the organization. (Stoneburner 2002.)

5 INFORMATION SECURITY POLICIES

Policies are a set of guidelines that describe an agreed procedure of dealing with a problem or difficult situation. They offer procedural instructions for employees and workers to follow should such an incident arise. Additionally, it outlines the rules of handling information assets; what is acceptable and what is not acceptable. An organization's policies must be contained in a well written document and must be communicated to all concerned personnel. Although every organization's policy document is ultimately unique due to unique business objectives, international standards like ISO 27002 offer a model structure of an organization's policy document. (Danchev 2003; Wood 2005.)

5.1 Importance of security Policy

The main aims of establishing a security policy are to ensure proper information security foundations, to describe the roles and responsibilities of the staff members in the protection of information assets and to demonstrate the importance of securing the organization's communications. Creating a security policy is the first step towards mitigating risks associated with unacceptable use of the organizational information assets. Having a security policy not only fully engages the staff to participate in the organization's efforts to protect its information resources but also decreases the risk of a security breach caused by "human-factor" errors. The process of developing a security system enables the identification, definition and documentation of the organization's vital assets and how they should be secured. It provides for a centralized document with all information pertaining security of information resources. (Danchev 2003, Greene 2014.)

5.2 Information Security Frameworks and Tools

As mentioned earlier, there are accessible internationally recognized policy templates that can be emulated while developing an organization's information security policy document. Theses templates are innately for universal purposes and are not company specific. They should therefore be combined with management participation to produce a document specifically suitable for the organization. (ISO/IEC 27002 2013.)

5.2.1 ISO 27000

ISO (International Organization for Standardization) is a family of standards that provides organizations with a general framework for information security policies and standards. This series is useful to every organization that wishes to secure information assets such as financial reports, employee information, intellectual property or customer details. The ISO 27000:2013 is a series consisting of four standardization documents. Firstly, the family contains the ISO 27001:2013 that contains the requirements for an information security management system. ISO 27002:2013 is the second document in the series and contains a list of code of practices that ensure security. The third document in this family is ISO 27003:2010, which is designed to provide guidance during the implementation stage of the security management system. Fourth on this series is ISO 27004:2009 that encompasses the analysis of measurements required for an information security system (Karjalainen 2014.)

ISO 27001:2013 is the standard adapted to offer guidance through the processes of establishment, implementation, maintenance and continual improvement of the information security management system. The standard considers various types of organizations and industries encompassing their sizes and markets. It is therefore a wide and generic document and its adoption and implementation ought to be a strategic decision. The standard's adaptation process must be influenced by the organization's needs, and aligned to its business objectives. The board and the executive management are at liberty to select

the security policies that are appropriate for the current state of security and may complement these policies with more options also referred to as extended control sets. Thorough evaluation of the organization's information security risks is fundamental in order to make suitable selection of controls. (ISO/IEC 2013, Henning 2009.)

ISO 27002:2013 is mainly a code of practice and categorically deals with all types of information security and not only IT systems' security (ISO/IEC 27002 2013). It offers guidelines and recommendations of suitable controls to organizations that have assessed their information security risks. Since it is a code of guidelines, organizations are not necessarily required to adopt it as a standard and are therefore free to choose guidelines that are relevant to their organization's needs. This standard is considered indispensable to any organization that depends on information. (ISO/IEC 27002 2013.)

ISO 27003 was formulated as an implementation guide for organizations that have chosen to implement the ISO 27000 standards. It provides guidance in the initiation stage of ISMS development, precisely in the specification and design phases. ISO 27004 provides support to organizations in the assessment phase of the ISMS. An organization with implemented ISMS needs to regularly conduct evaluation checks in order to certify that the security requirements have been satisfied. The standard helps to define metrics and measurements that determine the competence of ISMS and makes an analysis with the aim of improving its effectiveness. Measurement results aid in making both business and engineering decisions regarding information security. (ISO/IEC 2013.)

The ISO 27000 family of standards provides a comprehensive framework for the development of security policies, controls and management systems. An organization does not need to adopt all the policies included in this family of standards. The main idea is to comprehend the domains that are applicable to the organization and then proceed with adapting the controls in the development and implementation processes. It is important to remember that policies should support and not frustrate the goals and objectives of an organization. Ultimately, the success of an information security project depends on a combination of management's commitment and a project manager with sufficient understanding of the organization's objectives and security needs. (Henning 2009.)

5.2.2 NIST

The US National Institute of Standards and Technology (NIST) is prominent for developing extensive and comprehensive standards. NIST has a department known as the Computer Security Division whose mission is to promote information systems' security. The department has taken upon itself to raise awareness on the vulnerabilities and risks that information technology organizations face. It conducts research and studies on cost effective security and offers advice to organizations. Subsequently, NIST develops controls, standards, policies and validation programs to promote security among consumers and determine minimum security requirements. More than 300 security related documents have been published by NIST. Special Publication (SP) 800 series is a part of the comprehensive research and documentation completed by the institute. By developing guidance issues, materials, documents and advice pertaining information security, NIST successfully accomplishes its mandate and mission to the extent of serving governments, industries and academic institutions. (Greene 2014.)

5.2.3 ITIL

ITIL (Information Technology Infrastructure Library) is a compilation of best practices for IT organizations' management. ITIL aims at ensuring that strategic security considerations are taken at various operational levels. Information security is viewed as a cycle which needs to be controlled, planned, designed, tested and maintained. According to ITIL, information security is broken down to policies, processes, procedures and work instructions. Using ITIL as a guiding tool, organizations are able to develop and implement a clear security structure based on best practices. One of its requirements is continuous review and this ensures that an organization evaluates the effectiveness of its security measures. The security structure is well organized and therefore prevents disorganized implementation and rushed decisions. ITIL requires proper reporting and therefore keeps

the executive management up-to-date with the current security situation that enables them to make appropriate security decisions. Roles and responsibilities are clearly spelt out and in the event that an incident occurs, the procedures of action are understood. (Weil 2010.)

5.2.4 COBIT

COBIT (Control Objectives for Information and related Technology) is a governance framework established by ISACA (Information System Audit and Control Association). ISACA defines information security as an entity that ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability). COBIT 5 for Information Security complements the COBIT 5 framework by creating equilibrium between attaining benefits and maintaining optimal risk levels and resource use. It enables clear distinction between governance and management by clearly explaining how the duties of governance differ from those of management. COBIT, in its principles, emphasizes the importance of including all stakeholders and third parties in the organization's information security structure and clearly defining their responsibilities. COBIT 5 for information Security has a structure that consists of principles and enablers. The principles ensure effective governance and management while the enablers provide for optimal use of resources taking into consideration enterprise's and stakeholders' benefits. (ISACA 2012.)

6 INFORMATION PROTECTION

Until two decades ago, information protection was an easy task since computer systems and information infrastructure were located behind closed doors with very limited access. Today, it is a complicated and ambiguous task. Information infrastructure comes in different forms from large supercomputers to handheld and portable devices. Other forms of information systems are cloud based storage systems which have taken computing and information processing to a new level and in turn raised the information security standards. (Greene 2014.)

6.1 Physical Protection

Most managers and security professionals concentrate more on technical issues of information security neglecting physical protection. Physical access can be the least complicated way to gain access to information. Physical protection should therefore be considered elementary and essential. It involves setting up security infrastructure and barriers that prevent physical entry by unauthorized persons. (Greene 2014.)

6.1.1 Cabling

Cabling security seeks to safeguard any cable that transmits data or offers support to information services from tapping or damage. Parts of the recommendations made by ISO 27002 require implementation during the construction of the building. Power and telecommunication cables should be laid underground and where this is not possible, the cables should be subjected to further adequate protection methods. Tighter measures should be considered where highly sensitive data transmission is involved. A utility company should be allowed to handle critical telecommunications cables for extra protection. Handling of cables in workstations should also be taken into consideration.

Cables should not be left hanging and should be protected from tangling that would cause breakage. Cables should be tied and placed away from the working area. Where possible, desks designed to handle cables should be fitted. Power cables and communication cables ought to be separated to prevent interference and also to minimize the risk of losing or damaging both concurrently. Routes that pass through public areas should be avoided especially for network cables. Conduit should be used to protect network cables. (Calder & Watkins 2008.)

6.1.2 Protective rooms for devices

Areas and that contain information processing and support equipments within an organization are required to have a secure perimeter. A perimeter is defined as an object that forms a barrier to the entrance or separates the organization from the outside world. It includes but not limited to walls, doors, gates, floors and ceilings. The perimeter should have a faultless perimeter without gaps or weaknesses. Special attention should be given to lifts, risers and lift shafts where access can easily be gained by intruders. A reception that is always staffed is encouraged as it ensures authorized access to the premises and control of visitors. Doors and windows should be locked whenever the room is unattended. Extra protection should be fitted on the entrances and doors such as burglar bars, alarms and CCTV cameras. When the organization is engaged in highly confidential work, supplementary security may be considered. (Calder & Watkins 2008.)

6.1.3 Access control

Access control is a security measure that ensures protection of information from unauthorized persons and allows authorized users and systems to interact and communicate. The principal purpose of access controls is to protect data, information and information systems in order to ensure their confidentiality, integrity and availability.

Access controls offer protection from unauthorized access, modification or disruption. Access control systems are characterized by an identification scheme, authentication scheme and authorization scheme. Identification is the process of supplying the system with unique user details Authentication refers to how the user credentials are validated. Authorization allows access into the system. Access controls could be technical where firewalls or passwords are used for authentication, or physical such as the use of locks to deny access unless authorized. For authentication to take place, it is necessary that the user provides their unique credentials. The credentials can be knowledge credentials requiring information that the user knows for instance, a password. Possession credentials involve something the user has for example, a memory card. Biometrics is also a method of authentication where the user's inherence is used. It involves something that the user is, for example, fingerprints or DNA. (Greene 2014.)

6.2 Administrative works

Administrative works are the duties and responsibility carried out by the people working within the organization. This section has responsibility to be carried in order to run organization smoothly. These different sections are defined and briefly described in the following paragraphs. (Pineda 2010)

6.2.1 Training

It is a process of teaching or developing the skills and knowledge of the member staff working for certain organization which relate to few useful competencies. Training is peculiar objective of developing one's capabilities and performance. Different organizations have various security management skills and strategies .Therefore, it is very essential that every member of the organization must be aware about the information security system to maintain privacy and avoid accidental loss of data. (Pineda 2010.)

6.2.2 Secure Business Rules

The contracts formed by the organizations must implement the specifications that business associate must have administrative, physical, and technical safeguards. These specifications must be reasonable and relevantly protect the confidentiality, integrity, and availability of the electronic protected information that it creates, receives, maintains, or transmits. They should also ensure that any agent, including subcontractor, to organization it provides such information agrees to safeguard the information. Reports should be delivered to cover presence of any security incident of which it becomes aware. Covered security incidents may already have business associate contracts in place in order to comply with the Privacy Rule. If the business associate creates, receives, maintains, or transmits EPHI, these existing contracts should be reviewed and modified in order to meet the Security Rule Business Associate Contracts requirements. Alternatively, covered security incidents could have two separate contracts to address the requirements of the Privacy and Security Rules respectively. (Berson & Dubov 2008.)

6.2.3 Access control to Networks

A computer network solution for security access. It helps to enforce user authentication and network security. In brief when a computer is connected to a network it is not permitted to access network unless it is provided with user authentication, certain antivirus protection level, system update level and configuration. The computer is able to access only when it meets the policy and requirements. Networks access control is mainly used in endpoints checks. For example, in an organization the financial department could only access Finance department files if both the role and the endpoint meets anti-virus minimums. (Rouse 2015.)

6.2.4 User's authentication

The process that determines whether the information given is authorized information in the database. If the credentials match, the user can continue to process further. User authentication is identified in the human-to-computer interactions other than the guest accounts. (Rouse 2015.)

6.2.5 Decentralization of Administration

The process of division or dispersing of functions, powers, people or stuff away from a central location or authority into small parts or division is called decentralization of administration. This kind of structure is practiced in many of the organizations in order to be up-to-date with their day-to-day activities. (Decentralization Thematic Team 1997.)

6.3 Data and Networks protection

Security issues are the most complex issues in a network environment. It is very essential to ensure that access to the network is controlled, and data is safe enough from the attacks during the transmission across the network. There are many technologies which helps organizations to maintain their privacy and integrity (Greene 2014.)

6.3.1 Backups

Sensitive data is the heart of every organization. And to protect this sensitive data organization should implement data backup and recovery plan. Accidental data loss, database corruption, hardware failures and even natural disasters can be controlled. It is the

responsibility of the information security management to confirm that backups are made and located in a safe location. Various organizations might use various types of backup techniques according to the kind of data. The backups may be normal, copy backups, differential backups, incremental backups and daily backups. There are also different backup devices. (Rouse 2015.)

6.3.2 Secure Remote access

In this world of business, it is demand that offices are not defined in a certain place. The organization requires tools that will allow their employee to access to their corporate resources not only from their offices but also any device and place. Many organizations protect their sensitive data using corporate network and turning to an SSL VNP solution for remote access. The demand of flexibility of working environment needs quick access to critical business applications and data from anywhere. Information security management should ensure that the remote access solution is secure and protects sensitive information safely. (Microsoft 2013.)

6.3.3 Secrecy of Information

This is the practice of hiding sensitive information from certain personnel or groups, maybe sharing this kind of information with other may cause great loss to the organization. Secrecy of information has become a vital part in protection of data. The leakage of any information from an organization may benefit the rivals and it brings lot of damages to the organization reputation. Therefore, all the sensitive data should be encrypted and should be accessed to only few persons who are trustworthy. (Adam 2004.)

6.3.4 Firewall

This is a network security system that controls the unauthorized accesses to a private network. It can be installed in both hardware and software in order to protect data. It helps to eliminate possible weak points. To eliminate potential weak points in the network infrastructure; you may opt to pass data from protocol to protocol without the complexity of decryption and re-encryption. To do so securely, you must have some way to securely transfer data across network protocol boundaries. The internet enables connection of corporate intranet to a broad public network. Although this capability provides enormous business advantages, it also entails the risks to data and computer system. One way of protecting the privacy and integrity of your system is to place a firewall between the public network and your intranet. (Microsoft 2014.)

6.3.5 Anti-virus protection

Antivirus software refers to a computer program which is aimed to examine the files in order to detect and remove computer viruses or other malicious objects. The aim for using antivirus protection is to scan the computer in order to found out if it is infected with any form of malicious viruses which helps in breaching the security of the system or slowing down the performance. If any form of malicious attack is found, the antivirus program warns the internet about the attack and asks for further action, either to delete data or keep data. It also helps to deal and protect the user with the spyware and adware, two vices of the modern world. (Microsoft 2013.)

6.3.6 Inspection of communication

Inspection of communication should be made in every organization to check whether the sensitive information has been stolen or shared with the third parties. It necessary to keep

track of the communication if the data while being sent is stolen or forwarded to the wrong person. This might harm the organization and bring ubiquities. (Bakar, Hassan, Mustaffa & Che 2013.)

6.3.7 Intrusion observation

It is a type of security management system for computers and networks. An IT system gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusion an extrusion i.e. attacks from outside the organization. ID uses vulnerability assessment sometimes referred to as scanning, which is a technology developed to accesses the security of the computer system or network. (Frincke 2002.)

7 DAY-TO-DAY ACTIVITIES

An organization that has successfully conducted a risk analysis, established sound security policies and an information security management system has a solid foundation for creating a secure working environment. Enforced and implemented security policies direct the daily activities in an organization where roles and responsibilities are clearly understood. At this point, the board and executive management should demonstrate their commitment and provide tangible support to the other staff members and employees. (Burgess & Power 2008.)

7.1 Information System's Inventory

In addition to ensuring security in the daily activities, an organization ought to have a comprehensive and up-to-date inventory of its information assets. An information assets inventory has major benefits including business valuation and insurance coverage. Both hardware and software assets should be accounted for. Hardware assets include all the tangible equipments and information storage media. All programs and code that provide an interface between the hardware and the user should be classified under the software assets. The operating system, productivity software and application software comprise the software assets category. With this arrangement in place, it becomes easier to maintain a record of the persons responsible for particular assets. Daily management of the assets and accountability is therefore ensured. An inventory also ensures that cases of damage, loss or misplacement of assets are discovered early enough for proper remedies to take place. An asset's disposal or destruction should be handled with extreme care and properly documented. (Greene 2014.)

7.2 Human Resources Security

While it is a common belief that people are the most valuable asset in an organization, personnel can also be a resource of immense threat. It is probable that an employee, who is the "authorized person", can become the malicious attacker. Many technology professional are focusing on ensuring security on their network and are disregarding the possibility of internal attacks (Durgin 2007). Before an employee is granted access to an organization's information system, background checks must be conducted in order to know their level of education, weaknesses and criminal records. The employee must also go through an orientation in order to learn about the organization, the job and its responsibilities. The employee should also agree to sign an employee contract and confidentiality agreements. Termination of an employee's contract is viewed as the most dangerous stage. This is true depending on the circumstances surrounding the termination. A disgruntled employee leaves an organization with a feeling of outrage. Unknowingly, most managers are relieved and relaxed once the employee leaves not knowing that they will seek retribution for their feeling at a later date. (Greene 2014.)

7.3 Information security Culture

An information security culture is viewed as a combination of beliefs and values that direct the activities and behavior of employees in an organization (Fagerström 2013). It is a perception of the practices that are acceptable and those that are unacceptable as far as information security is concerned. A security culture ought to offer support to all ventures in order for security to be a usual practice in everyday activities in the organization. An information security culture is essential in carving the behavior of employees towards security consciousness. Management's attitude and commitment towards information security is largely reflected by the organization's information security culture. Training and awareness programmes coupled with management's commitment facilitate the development of the right security perceptions among employees hence influencing their view of information security. (Durgin 2007, Fagerström 2013.)

An appropriate information security culture within an organization helps to create a secure environment. This is because employees will not hesitate to perform their tasks securely therefore increasing security precautions. When these security activities are performed on a daily basis, they become the organization's norms consequently making a secure environment everyone's priority. (Zakaria, Gani, Nor & Anuar 2007.)

8 OBSERVATION OF CHANGES AND MAINTENANCE

In today's time an organization mission is critically dependent on the environment of the information technology, the ability to manage this technology and safeguard the sensitive information is also a crucial task. An organization needs a god IT infrastructure where it meets the needs of its regulatory structure, missions, and core business process. Information security process should proactively manage to identify new threats and respond to vulnerabilities with the constant changes in architecture and operational environment. As the risk management structure describes a structure process that helps to arrange information security and risk management activities into the system development. As the technology is evolving rapidly, therefore a very deep observation should be made on the architecture of the information security. (Dempsey et al. 2011.)

The observation of the security system can be made by collecting the documented report from ISMS. This document is the evidence of the process steps specifically involved in IT audits. This audited document can be in different format as the security policies varies from organization to organization. But the main aim is to get information of the entire scenario which was occurred during the whole process. The changes in the environment of security process can be observed step by step process. The very first step is to find the scope for the observation which is directly related to the organization. The auditor is the responsible person for this task. They should also give particular attention to the information security risk and control associates. The possible outcomes from this process are scope, charter and engagement letter, auditing working papers, evidence and reports. (Dempsey et al. 2011.)

The work plan is made by breaking the scope into smaller parts for the greater detail of the certain areas. The time and the resources are negotiated by the management of the both organization and ISMS auditors in the form of audit plan. The project planning techniques such as GANTT charts are usually used. The plan also include "checkpoint" that is specifically made by auditors to inform updates to the management if there occurs any notification of potential threat. The auditors are independent from the organization for the

investigation of events which make a cooperative environment to gather information that represent greater risk to the organization. The output from this process is the audit work plan agreed by the management. (Dempsey et al. 2011.)

During the field work phase, audit evidence is collected by the auditors working methodically through the work plan. For example, interviewing staff members, managers and other stakeholders associated with the ISMS, reviewing document, data, observing ISMS processes in acting and checking system security configurations. Various tests are performed in order to validate the evidence if it was true or false. The first part of this phase is to review the documentation made by ISMS. The auditors make a note about the documentation formed by the ISMS such as applicability, risk treatment plan and ISMS policy. Findings from the documentation review give us the information about the need of the audit test to recognize how deeply the ISMS follows the documentation, as well a general level of test are done to check the appropriateness of the documentation in relation to ISO/IEC 27001. IT systems are tested by using compliance technical test to verify if the organization has configured those systems in accordance to the information security policies, standard and guidelines. (EPA Information Procedures 2014.)

Analysis is made on the gathered audit evidence; documents are reviewed and verified in relation to the risk and control measures. It helps the organization to identify the gap between the evidence and notifies the need for additional audit test, where further work may be required. The main aim of analysis is to prioritize the attention towards the risk where it is most important. The most important part of the observation process is reporting which itself has the sub-process. A typical ISMS report contains the title, introduction, name of the organization, clarifying the scope, objective period of coverage and the environment, time and period of audit plan performed. It also contains detail finding and analysis, problems recommended and evidence, of the event which may have potential risk to the organization. Hence, the final output is the audit report of ISMS which is signed with date and distributed according to the terms of the audit charter. The final phase is the closure phase where the entire audit files are closed. It contains preparing notes for future audits and plans to check the agreed actions to be completed on time. When all the mandatory audit recommendations are completed and satisfied by the auditors, the

organization's ISMS certificate is prepared and published. (Dempsey, Chawla, Johnson & Johnston 2011.)

Maintenance is the process to maintain the established security system. We all know IT is evolving day-by-day. It is almost impossible to imagine a stable security system without security maintenance. The staff members, managers, the organizations should be aware of the security management system to avoid any vulnerabilities. The security maintenance procedure varies according to the security policies and standard that the organization has. There are different areas in the organization security management system where up-to-date maintenance is needed. The system maintenance policy and procedures help to develop and disseminate periodic updates. A documentation of the facilities implemented in the information system maintenance policy and it controls is made. Periodic maintenance is a type of maintenance which schedules, performs and documents routine preventive and regular maintenance to the components of the information accordance with the manufacturer or vendor specification. (EPA Information Procedures 2014.)

Maintenance tools are approved and monitored for maintenance of information security tools. Maintenance verifies whether the tools contain any malicious code that may harm the system. Also it is important to checks if the maintenance of the tools is made by authorized person to avoid any likelihood in the security system. Remote maintenance is another very sensitive process which controls, approves and monitors the remotely diagnostic activities. The organization describes the use of the remote diagnostic tool in the security plan for the information system. The organization maintains maintenance logs for all the remote service activities. Personnel maintenance controls that only authorized personnel perform maintenance on the information system. Finally, timely maintenance which supports to meet the business availability requirements should also be ensured. Thus these are the maintenance process which makes every organization information security system up to date. Nonetheless, it also minimizes the unexpected threats or vulnerabilities to the organization. (EPA Information Procedures 2014.)

9 CONCLUSION

Following the pervasive application of information and communication technologies, ICT systems are now the basic core and reservoir of all pieces of information that are fundamental to organizations. In recent times, the interconnected information systems and networks drove the organizations into a critical situation that determines the need of explicit measures for information protection. On one hand, ICT systems are becoming more and more complex with advancement in technology. On the other hand, launching damaging attacks against the systems requires less complex skills. Information security has never been more important than it is today. Today's threats cannot be countered with yesterday's strategies. Organizations need a current and well established model of information security architecture, one that is driven by knowledge of threats, assets and the motives and targets of potential adversaries.

From the literature review and all the collected information denotes that, every organization must establish an adequate space for information security management policies, practices, risk management, observation and maintenance along with the day-to-day activities to long term activities to address the technical and non-technical aspect of ISMS. ISO has identified several frameworks, standards and models such as ISO27001. COBIT and OCTAVE is also used to align information technology for the continuity of the business. Information technology laws and regulations help to protect data and also the misuse of protected data. Although there are a number of security standards implemented in the organization properly, but still it cannot be protected fully because of the third-parties involvement in the organization. Senior managements, information security practitioners, IT professionals, auditors, staff members and the users all have a vital role to play in safeguarding the assets of the organization. This can be performed by providing awareness about the importance of the security system and its value. Only the cooperation at all levels of an organization, both internally and externally involved members might bring a safe and secure environment for the information security.

REFERENCES

Bigioni, P. The ICT security issues and trends. Available: http://www.forumti.it/fti/downloads/Summary_OCI_04.pdf . Accessed 14. April 2014.

Burgess, Christopher & Richard, P. 2008. Secrets Stolen, Fortunes Lost. Burlington: Syngress Publishing, Inc.

Calder, Alan & Steve Watkins. 2008. IT Governance : A Manager's Guide to Data Security and ISO27001/ISO27002. London: Kogan Page Limited.

CISSP. 2006. CISSP Guide to Security Essentials. Boston: Cengage Learning.

Danchev, D. 2003. Building and Implementing a successful Information Security Policy. Windowsecurity.com. Available: http://www.windowsecurity.com/pages/security-policy.pdf. Accessed 10 April 2015

Decentralization Thematic Team. The Online Sourcebook on Decentralization and Local Development. Available: http://www.ciesin.org/decentralization/English/General/Different_forms.html Accessed 25. April 2015.

Dempsey, K., Chawla, N., Johnson, A. & Johnston, R. 2011. Information Security Continuous Monitoring (ISCM) for Federal Information. NIST Special Publication 800-137.

Durgin, M. 2007. Understanding the Importance of and Implementing Internal Security Measures. SANS Institute. Available: http://www.sans.org/reading-room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures-1901. Accessed 15. April 2015.

Extreme Networks. Network Access Control. Available: http://www.extremenetworks.com/product/network-access-control Accessed 25. April 2015.

Fagerström, A. 2013. Creating, Maintaining and Managing an Information Security Culture. Bachelor's thesis. Arcada University of Applied Sciences. Degree Programme in Information and Media Technology.

Frincke, D. 2002. Intrusion Detection. IOS press Inc.

Greene, S. 2014. Security Program and Policies: Governance and Risk Management. Available: http://www.pearsonitcertification.com/articles/article.aspx?p=2192704&seqNum=2 Accessed 14. April 2015.

Greene, S. S. 2014. Security Program and Policies: Principles and Practices. Indiana: Pearson IT Certification.

Henning, D. 2007. Tackling ISO 27001: A Project to Build an ISMS. ISO27k Information Security Standards. Available: http://www.iso27001security.com/GIAC_GCPM_gold_henning.pdf. Accessed 14. April 2015.

HHS.gov. Health Information Privacy. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html Accessed 24. April 2015.

Humphreys, E. 2010. Information Security Risk Management. London.

ISACA. 2012. COBIT 5 for Information Security. Available: https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf . Accessed 20. April 2015.

Iso27001security. 2013. ISO/IEC 27002. Available: http://www.iso27001security.com/html/27001.html Accessed 20. April 2015.

ISO/IEC. 2013. ISO/IEC 27001:2013(en). Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. Accessed 20. April 2015.

Kajava, J., Juhani A., Rauno V., Savola, R. & Roning, J. 2006. Senior Executives Commitment to Information Security - from Motivation to Responsibilty. Oulu.

Karjalainen, M. 2014. Building an Information Security Management System. Bachelor's thesis. Laurea University of Applied of Sciences. Degree Programme in Security Management

Microsoft. 2013. Securing Remote Access. Available: https://msdn.microsoft.com/en-us/library/cc875831.aspx Accessed 25. April 2015.

Microsoft. 2014. Safety and Security Center. Available: http://www.microsoft.com/security/pc-security/firewalls-whatis.aspx Accessed 25. April 2015.

Online Trust Alliance. 2014. 2014 Data Protection & Breach Readiness Guide. Available: http://www.otalliance.org/resources/incident/2014OTADataBreachGuide.pdf. Accessed 14. April 2015.

Peltier, T.R. 2005. Information Security Risk Analysis. Newyork: CRC press.

Ponemon Institute. 2014 . 2014 Cost of Data Breach. IBM. Available: http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/ Accessed 20. April 2015.

PWC. 2014. Many are Defending Future Threats with Yesterday's Strategies, finds PwC, CIO and CSO's The Global State of Information Security® Survey 2014. Available: http://www.idgenterprise.com/press/many-are-defending-future-threats-with-yesterdays-strategies-finds-pwc-cio-and-csos-the-global-state-of-information-security-survey-2014-2 Accessed 30. March 2015.

Rouse, M. 2015. Essential guide to business continuity and disaster recovery plans. Available: http://searchsecurity.techtarget.com/definition/authentication. Accessed 25. April 2015.

Safety and Security Center. 2013. Available: http://www.microsoft.com/en-gb/security/resources/antivirus-whatis.aspx Accessed 25. April 2015.

SANS. 2013. Security Best Practices for IT Project Managers Avaialble: http://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257. Accessed 14. April 2015.

Stoneburner, G. Goguen, A. & Feringa, A. 2002. Risk Management guide for information technology. NIST Special Publication 800-30.

TISN. 2009. IT Security Governance - CIO, CISO and Practioner Guide. Available: http://www.tisn.gov.au/Documents/ITSEAG+IT+Security+Governance+paper+(Word).doc Accessed 21. April 2015.

Tung, L. 2014. IT security governance: Boards must act. Available: http://www.zdnet.com/article/it-security-governance-boards-must-act/. Accessed 14. April 2015.

Weil, S. 2010. How ITIL Can Improve Information Security. Available: http://www.symantec.com/connect/articles/how-itil-can-improve-information-security. Accessed 19. April 2015.

MindfulSecurity.com. 2009. Why is Information Security Important? Available: http://mindfulsecurity.com/2009/07/01/why-is-information-security-important/ Accessed 23. April 2015.

Wood, C. C. 2005. Information Security Policies: Distinct from guidelines and standards. Search Security. Available: http://searchsecurity.techtarget.com/feature/Information-security-policies-Distinct-from-guidelines-and-standards. Accessed 14. April 2014.

Zakaria, O., Gani, A., Nor, M. & Anuar, N. 2007. Reengineering Information Security Culture Formulation Through Management Perspective. Proceedings of the International Conference on Electrical Engineering and Informatics. Bandung.