ADDIS ABABAUNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESMENT OF INFORMATION SYSTEM SECURITY MANAGEMENT IN SELECTED PUBLIC ORGANIZATIONS IN ETHIOPIA: A GAP ANALYSIS

By

GETNET G/EGZIABHER

JUNE, 2020
ADDIS ABABA, ETHIOPIA

ADDIS ABABAUNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF INFORMATION SYSTEMS SECURITY MANAGEMENT IN SELECTED PUBLIC ORGANIZATIONS IN ETHIOPIA: A GAP ANALYSIS

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science and systems (*Information Systems specialization)*

By

GETNET G/EGZIABHER

June 2020

Addis Ababa, Ethiopia

ADDIS ABABAUNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF INFORMATION SYSTEMS SECURITY MANAGEMENT IN SELECTED PUBLIC ORGANIZATIONS IN ETHIOPIA: A GAP ANALYSIS

By

GETNET GBREEGZIABHER

Name and signature of Members of the Examining Board

Lemma Lessa (Ph.D.)	_____	_____
Advisor	Signature	Date
Temtim Assefa (Ph.D.)	_____	_____
Examiner	Signature	Date
Dereje Teferi (Ph.D.)	_____	_____
Examiner	Signature	Date

Declaration

This thesis has not previously been submitted for any degree and is not being concurrently submitted in candidature for any degree in any university. I declare that this thesis entitled "ASSESSMENT OF INFORMATION SYSTEMS SECURITY MANAGEMENT IN SELECTED PUBLIC ORGANIZATIONS IN ETHIOPIA: A GAP ANALYSIS" is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references and a list of references is appended.

Signature: _____

Getnet Gbreegziabher

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Lemma Lessa (Ph.D.)

Dedication

This thesis is dedicated to the loving memory of my great and lovely ***Father****,* ***GEBREEGZIABHER FIKRU****, Who raised me to love, courage, confident and attain, but did not live to see this success.*

Acknowledgements

My deep gratitude goes to the almighty God for giving me strength in any direction of my life.

I would like to acknowledge my research advisor Lemma Lessa (PhD) who gave me comments and helped me by guiding and giving valuable suggestions to realize this thesis.

My deep gratitude also goes to respondents who devoted a substantial party of their time in giving the necessary information to conduct this research.

Finally, my heartfelt thanks are also rendered to my families and friends for their support who initiated me and sacrificed their time to join and complete my graduate study.

Getnet Gbreegziabher

June, 2020

Addis Ababa, Ethiopia

Abstract

The purpose of this research was to evaluate the Information Security Sector management (ISSM) implementation and find the gap analysis in four federal public organizations in Ethiopia. This study examined the practices and implementation, the trends regarding ISSM with particular reference with MOFED, MOR, TECHIN, and ESSTI. In terms of research methodology qualitative approach and multiple case study approach was employed. In this study, both primary and secondary sources of data were used. Subsequently, key informant interviewing and document analysis and observation were used to collect data. Qualitative method used as data analysis techniques as well as the interview were mainly used. This study identified numerous and examined the gaps in ISSM implementation in practice in public sector in the organizations and the way forward. This study further, examined the repercussions based on international ISO standards. The finding of the study revealed that the general gaps in ISS, lack of experienced human resource in the field, unable to implement an IT system, lack IT policy, lack of training, lack of user side understanding Violating Rules and regulations.

Keywords: Information System Security, Information System Security Management, Information System Security Management Framework.

Table of Contents

List of Tables

List of Figures

List of Acronyms

APO	Align plan and Organize
BAI	Build acquire and Implement
CIA	Confidentiality Integrity and Availability
CSF	Comprehensive Security Framework
COBIT	Control Objectives for Information and
DSS	Deliver Service and Support
EDM	Evaluate Direct and Monitor
ENISA	European Union Agency for Network and Information Security
ESSTI	Ethiopian Space Science and Technology Institute
FIPS	Federal Information Processing Standards
FAIR	Factor Analysis of Information Risk
HITRUST	Health Information Trust Alliance
IBEX	Integrated Budget and Expenditure System
IS	Information Security
ISSM	Information System Security Management
ICT	Information Communication Technology
IFMIS	International Finance Information System
ITG	Information Technology Governance
ISG	Information Security Governance
ISO	International Standard Organization
ITIT	Information Technology Infrastructure Library
ISACA	Information System Audit and Control Association
MINT	Ministry of Innovation and Technology
MOFED	Ministry of Finance and Economic Development
MOR	Ministry of Revenue
MEA	Monitor Evaluate and Access
OCTAVE	Operationally Critical Threat, Asset and Vulnerability
NIST	National Institute of Standards
PCIDSS	Payment Card Industry Data Security Standards
SOA	Statement of Applicability
TECHIN	Technology and Innovation Institute

CHAPTER: INTRODUCTION

1.1 Background

Organizations have different assets; one of the assets is information. Information is value and more and more organizations have related that information security risks can have negative influence on business process continuity and public image, relations, can cause financial loss, data loss, and influence relations with clients or public. Information which is the most valuable asset in an organization is assumed as a critical resource, enabling the organization to achieve its given goals. An organization could have its information systems used for different purposes and is managed indifferent approach. Besides, the information system management differs from organization to organization and further the type of management differs from one to another dependent on the organization's behavior. However, there is ultimate goal of information security to protect the interest of those who depend on information technology and communication systems that contain information from harm or attack (Mehdi, Hamid &Hashim, 2012; Ejersaa, 2016)

The globalized and the today's modern time mostly termed "information era" gives meaning in particular context and uses information and knowledge as important assets. This important resource needs to be protected against an authorized access or manipulation of information, either in storage, processing, exchange by groups likewise users such as hackers, phishers, social engineers, viruses, and worms that threaten organizations on all sides, through intranet, extranet, and the Internet. Thus, it needs to be protected efficiently and seriously developing information security system strongly.

From the general realities and emphasis given to, information and communication Technology (ICT) is very important in public service reform and driven by growing concern that the drives management projects. On the other hand, the rapid advancement of information and communications technology (ICT) and the growing dependence of organizations on ICT continuously intensify concern on information security (Heru & Mohammad, 2018).Parallel to this; information security has become the most challenging issues of today's organizations. Thus developing such system has become one of the largely preferred systems in order to achieve the information system as well.

Information Security Management mainly concern with strategic, tactical and operational issues that surround the planning, analyses, design, implementation and maintenance of

organizations' information security programs. Subsequently, information security management activities should be driven by organizational objectives so that noresourcesareexpendedonsecuritywithoutanexplicitdocumentedunderstandingofhowit supports the organizational mission (Joobin & Gurpreet, 2007). Further, information security refers to the protection of confidentiality, integrity, and access to information (Omar et al, 2016).

Moreover; information security helps to protect organizations information, information facilities and supports application of appropriate safeguards, security guards, security supports helps the organization's mission by protecting its physical and financial resources, reputation, legal position ,and assets(Peltier,2005).In addition, Information security primarily aim of information security is to protect the organization and its assets against attempts of intrusion and corruption **(**Gebrehiwot,2018).In relation with information security financial services now a day have been threatened by numerous criminal actors like wise electronic criminals (Tibebe & Eskatnaf,2017)

Ethiopia, which had grappled to respond different development stages of information security management since the last decades have been establishment of financial security system. This relatively compared with other countries in the region have made many revisions and reform course. Based such reforms Ministry of Finance and Economic Development (Here after MOFED),The Technology and Innovation institute (TECHIN) , Ethiopian Space science and technology Institute were with different but intertwined strategic goal and mission. MOFED was established with the aim to control the financial system of the country. The aforesaid institutions have got different missions and objectives such as checking compliance of public organizations in the country whether they have permission to run their fiscal year budget or not as well as MOFED introduces new and efficient systems of utilizing resources to both federal and regional governments by allocating budget. In addition, it provides various public finance and procurement services to different public zonal offices. As a result, the strategy helps to reduce public resources wastage as expenses that could be incurred by various offices are avoided.

According to MOFED (2019) reports indicate that the it has been effectively and efficiently engaged in improving its activities, services and foregoing existing experiences and the accommodation of new working procedures that can facilitate the duties of the ministry have made it necessary to improve in the finance, procurement, and stock management system of

the nation from time to time (MOFED,2019). The MOFED has under gone major reforms and have established objectives such as: establishment of modern revenue assessment and collection system; and provision of customers with equitable services , voluntarily discharge to tax payers on tax obligations, enforcing tax and customs laws by preventing and controlling contraband as well as tax fraud and evasion, to collect timely and effective tax revenues generated by the economy, and to provide the necessary support to regions to harmonize federal and regional tax administration systems(MOR, 2019). To fulfill the above objectives of the ministry there are different systems are used and implemented. The second establishment the Technology and Innovation institute (TECHIN) funded was established in2011inAddisAbaba, under the MINT. It has the function of providing information to Support scientific and technological (Here after ST) activities in the country. TECHIN has published information on the financing of research and development and on the nature and progress of innovative projects, and a strategy was set to create the necessary conditions to encourage and introduce bibliometric monitoring of publications in ST. Additionally, the center has also provided ICT facilities including a digital library, a patent information system, an automated personnel management system, and S&T-relateddatabase.1

The other development took place is Ethiopian Space science and technology Institute establishment. It was established on October14,2016.The main objectives of establishment of Ethiopian Space Science and Technology Institute(ESSTI) are to enable the country to fully exploit multidimensional uses of space science and technologies; to produce demand based knowledgeable, skilled and attitudinally matured professionals in the field of aerospace science that enable the country to become internationally competitive in the sector; to develop and strengthen space science and technology infrastructures to speed up space science and technology development in the country; and enable the country to be robust contributor for the development of aerospace science and technology.

The establishment of the above four institutions was a phenomenal to the development of the economy of the country. This have paved the way for each of them to be connected very much with multi-dimensional sets of information systems that could largely contribute to the country's development at each level including various organizations working and connected all together for the same goal. Studies conducted in the areas of information security sector management (ISSM) by numerous scholars present indicate that the existence of gaps and differences in public organizations performances. Therefore, the purpose of this study is to

evaluate the new information systems security management (ISSM) framework in selected public organizations in Ethiopia and find out the gap existed in the above listed four organizations.

1.2 Statement of the Problem

As stated in the background of the study, Information security sector management is one of the determinant factors in proper and effective organizational management in order to bring development and achieve aspired principal objective. Information security management refers to the control that an organization needs to implement to ensure the safety of its information assets and resources (Ejerssa, 2016). In addition, ISM is a series of management activities driven by developments in the fields of corporate governance and related legal and regulatory areas as well as it is a process of the explicit inclusion of information security as an integral part of good organizational or corporate governance (Salahuddin,2011).Thus organizations need a systemic information security approach that is very supportive for the arrangement or structuring of information security components to apply information security in an effective manner to prevent risks in a given organization (Quingxiong& Pauline, 2008; Ejjerssa, 2016)

According to Eloff and Solms (2000), the aim of information security is to protect the information systems and establish a framework by which organization can run information system operations as they are expected. ISM focuses on minimizing the risks of information systems in the operations. Information security is the protection of information and its critical elements' (Whitman & Mattord, 2018). Consequently, different public and private organizations have begun to use information security management in order for arrangement or structuring of information.

Repercussions of information technology can affect assets of given organization at different sets. It could affect whether public or private organizations. Likewise, any other institutions public organizations have been implementing ISSM and accepted the advantage of it to protect their business and confidential information. The organizations have developed dependence on activities related as well as when this institutions or organizations' information system is not only safe but also not well protected, and then there will be a risk.

According to ITU (2018), report, Ethiopia is grouped under low Global Cyber-security Index scores. Hence, the insecurity of the internet further exposes institutions to undetected,

global, and virtually instantaneous attacks on internal systems and proprietary information (Amarachiet al., 2013).

Further, Ethiopia faces different kinds of information security challenges especially with developing threats in the region with different dynamisms. In Ethiopia, information security system management was conducted in different sectors like banks, insurance, universities because the communication and technological development have generated dependence on it.

Studies were conducted in the areas of information management by different scholars. Aychiluhim &Tibebe (2015) conducted on how to ensure the security of cloud computing in the public sector. Gebrehiwot (2018) also evaluated on the Ethio-telecom ISSM division where as Aychiluhim (2015) studied Internet banking, and Tibebe & Eskatnaf (2017)studied the ISSM maturity level of Banks in Ethiopia. (Tibebe et al., 2009).

Regarding the ISSM, two studies are conducted comparatively By Nebyou Ejerssa(2016) , Lemma Lesaa and Alemayehu Tsegaye(2019). Nebiyu Ejersa (2016) has conducted his scholarly study titled "*Assessment of information security maturity level on Ethiopian public universities*" and has found the result there are institutions without security policy and human security policies, cryptographies need improvement. The other lemma Lessa and Alemayehu Tsegaye (2019) has a conference paper titled "*Evaluation of the public value of E-government services in Ethiopian Court Case management System*." And their finding put direction for and asserted that the e-government services in Ethiopia there is no research on the public value that the e-government service made. The focuses of the above studies were not ISSM of public organizations in Ethiopia and to knowledge of the researcher, there are no studies conducted on the features of public organizations and results to solve security problems.

In addition to this, a study that analyses in this regard were not conducted in Ethiopian Federal institutions. The other reason why the student researcher chooses to conduct study in this area is existence of challenges in reports and annual reports made by different security institutions of the country. The annual report of the INSA (2019) indicated the existence of external and internal challenges. Established on the above justification, a current status of public organizations aforesaid in ISSM in the four public Organizations need to be studied and the gap should be reflected to .Thus the extent and reason of the problem on one hand

and differences and similarities, practices, opportunities and challenges between the public organizations in implementing ISSM on the other hand should be studied.

The research intends to evaluate the gaps in the Information Systems Security Management practice in public sector organizations. The study tried to answer the following interrelated questions:

- What are the major practices in the implementation of ISSM in the four public sectors?
- How should the ISSM practice in public organizations look like?
- What are the challenges in the information security management of the public organizations?

1.3 General Objective

The main objective of the study was to evaluate the gaps in the Information Systems Security Management practice in public sector organizations

1.3.1 Specific Objectives

- To examine the **c**urrent implementation of ISSM in the four public sectors
- To identify the basic requirements of ISSM in the public sectors.
- To show the technology facility to implement the ISSM.

1.4 Significance of the study

The study could be taken as modest contribution in security sector as well as could provide solutions Information System Security Management practice gaps in the public organizations in the study area. The findings of this study would help the four public organizations on how they are exercising ISSM. In addition, this helps to organize the importance of ISSM concern for all public organization in Ethiopia. The result could further increase awareness and serve as an input in policy formulation of the officials, Further the result of this research provides new finding of information security management grounded on the identified critical controls. It provides the compulsory concerns to be accepted by Ethiopian public organizations classify their security risk areas. In addition, it helps to take actions based on the recommendation of this study. In addition, it may serves as springboard for further and in-depth study in the domain area.

1.5 Scope of the study

Nowadays there are many studies conducted on the area of information management in Ethiopia. However, this study will assess the ISSM gaps in the, Ministry of Finance and Economic Development, Ethiopian Space science and technology institute, Technology and Innovation institute, and Ministry of Revenue.

1.6 Organization of the study

This research work organized in five chapters.

This study was organized in five distinctive chapters. The first chapter includes the background of the study, statement of the problem, the research questions, and objectives of the study, significance and scope of the research. In the second chapter, review of related literature dealing with different resources of with different sources and justifications for implement the study is included and others reviewed and discussed thoroughly to provide an overview and explore the topic. In chapter three the research design, source of data, sampling technique, research population, data collection methods, sample design, validity, reliability, data analysis and ethical consideration were discussed. In chapter four, the data presentation and analysis and interpretation of the collected data is described and discussed based on the research problem. In chapter five the conclusion and recommendations of the research finding were presented. At last but not list, the list of references, appendices and annexes and guidelines were attached at back of the research.

CHAPTER 2: LITERATURE REVIEW

2.1 Information Security

The global business is expanding rapidly due to the explosion of information and communication technology (ICT) innovations (Henderson & Venkatraman, 1999, Lu & Ramanurthy, 2011). On the other hand, organizations have been largely supported and accelerated by information Systems (IS). Moreover, Information Systems has become an integral part of everyday life in the home, businesses, public organizations, and non-governmental organizations. As a result, the reliability on information system brought increasing profitability, competitiveness, and efficiency to the user such as individuals, organizations. To the contrary, developing sensitive information, valuable assets and intellectual property in the organizations against external and internal attacks has daily become more sophisticated and their challenge is obviously challenging (Martin, & Rice, 2011)

Information security largely focuses on protecting information from a wide range of threats in order to ensure business continuity, minimize business risks, and maximize the return on investments and public organizations.

2.2 Development of Information Security

The information flow has tremendously increased in the past few decades and with the technological advancements, the management of the large volumes of data. With continuous improvement of IT and developed globalized business, and it is interacted with variety of topics like threats intelligence programs and so on and technological usage has introduced a new threat to the business in maintaining the secrecy of the information (Suganthy and Moinak , 2014).

There exists a misconception with the use of the terms, information security, information assurance, and computer security. The common goals of all these interrelated fields are in providing the three major security goals: confidentiality, integrity, and availability of information. (Suganthy & Moinak, 2014).

With the purpose of understanding changes occurring in Information security system management begins with computer security. Computer security is needed to secure physical locations, hardware, soft wares from threats that developed during the Second World War when the mainframes, developed to aid computations for communications code breaking in

the war were applied by experts and military participants in order to take advantage. Besides, multi levels of security implementations were applied to deepen and widen the system to protect mainframes and maintain the integrity of their data. Moreover; the economic development and progress, competition among countries led to the today's more complex highly integrated, highly secured, technologically sophisticated computer security which is more secured than of any time (Candiwan, Puspita ,&Nadiihaq, 2019) .The wave of the information security management has staged the fourth levels currently(Ejerssa, 2016). Supporting this, Ejersa(2016) explains that there are four waves of security .The first was technical in nature, the second wave was managerial and the third wave was institutional and the current one as said above is Information security governance.

Waves	Description	Identifying Issues
The Technical Wave Duration: up to about the early 1980s	This wave is mainly characterised by a very technical approach to information security.	Access control lists, user-IDs and passwords.
The Management Wave Duration: from about the early 1980s to the mid-1990s	This wave is characterised by a growing management realisation of, and involvement with, the importance of information security. The Management Wave supplements the Technical Wave.	Information security policies, information security managers and organisational structures for information security.
The Institutional Wave Duration: started in the late 1990s	This wave is characterised by the development of best practices and codes of practice for information security management, international information security certification, cultivating information security as a corporate culture, and dynamic and continuous information security measurement.	Information Security Standardisation, International Information Security Certification Cultivating an information security culture right throughout an organisation. Implementing metrics to continuously and dynamically measure information security aspects in organisations.
The Governance Wave Duration: continues today	This wave is driven by developments in the fields of Corporate Governance and related legal and regulatory areas. It therefore can be described as the process of the explicit inclusion of information security as an integral part of good corporate governance, and the maturing of the concept of information security governance into the business mainstream.	Management and leadership commitment of the board and top management towards good information security; proper organisational structures for enforcing good information security; full user awareness and commitment towards good information security; and necessary policies, procedures, processes, technologies and compliance enforcement mechanisms.

Figure 2: The ISMS Waves description and issues Source: (Salahuddin, 2011).

2.3 Information System Security

Information is value, and as described in the background too many organizations have realized that information security risks can have a negative influence on business process continuity and public image, relations can cause financial loss as well as create problems (Whitman & Matoord 2008). Information security is the protection of information and its

critical elements (Ibid). Information security has three main characteristics: They are confidentiality, integrity and availability. And they are the CIA Triad of information security (Kreicberga, 2010).

The purpose of information protection is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization meet its business objectives or mission by protecting physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets (Peltier, 2005).

Information protection is a means to an end and not the end in itself and it supports the business objectives or mission of the enterprise. In business, having an effective information protection program is usually secondary to the need to make a profit. In the public sector, information protection is secondary to the agency's services provided to its constancy (Colley, 2007).Information protection is an integral element of due care which needs to be cost effective and controls can be based on proposed with necessary to confirm that significant risks that exists. Moreover, Information protection responsibilities and accountabilities should be made explicit. For any program to be effective, it will be necessary to publish an information protection policy statement and a group mission statement. System owners have information protection responsibilities outside their own organization. Access to information will often extend beyond the business unit or even the enterprise.

Information protection requires a comprehensive and integrated approach. To be as effective as possible, it will be necessary for information protection issues to be part of the system development lifecycle. Information protection should be periodically reassessed. As with anything, time changes the needs and objectives. Information protection is constrained by the culture of the organization. The ISO must understand that the basic information protection program to be implemented throughout the enterprise.

Further, information security has been considered to be mainly a technical field of any decades, and the management of information security is interrelated with human factor. Senior management is charged with two basic responsibilities: a duty of loyalty this means that whatever decisions they make must be made in the best interest of the enterprise.

According to the Peltier (2005), from the above elements security policy is the first and probably most important aspect of information security. Policies become the core of information security that provides a structure and purpose for all other aspects of information security train and he pictured it as follows.

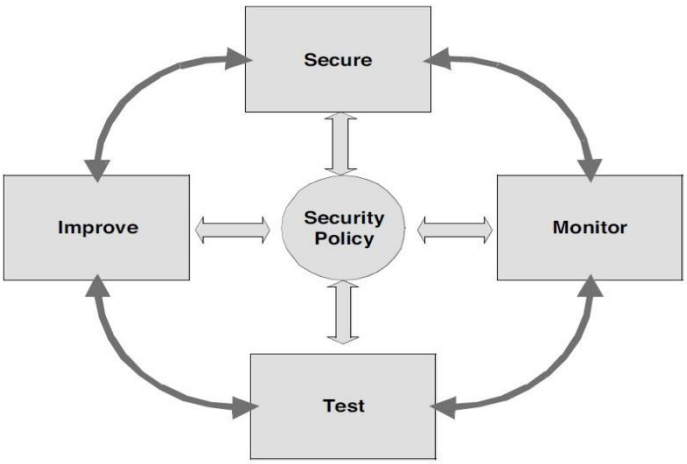

Figure 1: Security Wheel. Peltier (2005)

2.4 Information Security Governance

Information security governance consists of the leadership, organizational structures, and processes that safeguard information. In addition to critical to the success of these structures and processes is effective communication among all parties based on constructive relationships, a common language and shared commitment to addressing the issues.

According to IT Governance Institute (2006), as information and information technology are of increasing strategic importance, effective management of IT and information assets has become acritical strategic concern. In addition, IT Governance (ITG) deals with the management of an organization's use of IT (Janneet al., 2012). According to the aforesaid Institute (2007), it is "*an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives*".

Effective information security governance can integrate legal, managerial, operational, and technical considerations. It shall specify roles that have the requisite authority, accountability, and resources to implement and enforce policies, standards, awareness programs, security strategies, and other organizational procedures. Thereby, it establishes an appropriate framework for decision making that relies on well-informed decision-making and ensures that decisions are enacted, implemented and monitored consistently (Janne et al.,2012).ISG framework and function model should be consistently constructed with other corporate risk governance framework so that executives can make decisions easily and

effectively, since information security is one of the major corporate risk areas, and management of information security risk also should be a part of corporate risk management framework. Besides, ISG function model also needs to be capable to handle unique characteristics of information security risk, which are essentially different from other risk categories. It further, ISG functional model should be able to include existing information security management and control mechanisms, such as ISMS and be able to have an effective interface with the elements of these existing mechanisms.

2.5 Information Security Management Process

Information process management characterizes the process of personnel leading and directing all or part of an organization through a deployment and manipulation of resources likewise human capital, natural, intellectual or intangible (Ejerssa, 2016). This process has different models and this is an iterative planning process specification and design from inception to the production of implementation plans. Documentation and records control process is the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS **(**KnutHaufe etal., 2016). Its main goal is provide confidence, which the security requirements that have been executed on the system are adequate to protect data and resource.

As it is known information use is growing rapidly in unprecedented ways and there is large need for information safeguard and management in efficient and effective order by corporations, public organizations, government institutions, non-profit organizations (Betrand, 2012).The following table shows the overall information security process.

Table 1: ISMS Processes (Knut Haufeet., al2016)

S.N	Process/criteria	Process category
1	ISMS planning process	Management process
2	Information security governance process	Management process
3	Information security risk assessment process	ISMS core process
4	Information security risk treatment process	ISMS core process
5	Resource management process	ISMS core process
6	Process to assure necessary awareness and competence	ISMS core process
7	Communication process	ISMS core process
8	Documentation and records control process	ISMS core process
9	Requirements management process	ISMS core process
10	Information security change management process	ISMS core process

11	Process to control outsourced processes	ISMS core process
12	Performance evaluation process	ISMS core process
13	Internal audit process	ISMS core process
14	Information security incident management process	ISMS core process
15	Information security improvement process	ISMS core process
16	Information security customer relationship management process	ISMS core process
17	Configuration management process	Support process

2.6 International Standards of ISSM

Quite a lot of common security control frameworks are being used by a number of businesses or organizations protect against vulnerabilities, and choosing the right framework depends on several factors specific to MSPs and their clients.

An information security framework is asset of documented, agreed and understood policies, procedures, and processes defining the ways information are managed within a business organization. The main target is to lower the risk and number of vulnerabilities and increase confidence throughout the organization.

Security Framework is a risk-based approach to reduce cyber security risks. It is composed of following parts. The Framework Core, the Framework Profile, and the Framework Implementation Tiers or the “Cyber security Framework” (The National Institute of Standards and Technology, 2002). In the same vein, framework core consists of four different element types: Functions, Categories, Sub categories, and Informative References. The Core presents industry standards, guidelines, and practices allowing communication across the organization from the executive level to the operative implementation level (Henttinen, 2018).

Additionally, Framework Profile is the representation of the outcomes from Framework Categories and Subcategories that a particular system or organization has selected. It can be characterized as the alignment of standards, guidelines, and practices in a particular implementation scenario. The existing organization security posture can be improved by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state) (Henttinen, 2018).

By developing a Profile, an organization can review all categories and eight sub categories and, based on a risk assessment and information on business drivers, determine the most important ones for the organization. Categories and sub categories can also be added to better

address the organization risks as well as support the prioritization and measurement of progress to ward the Target Profile. Profiles can be used as self-assessments and communication with in and outside the organization. The current profile can be used to support the planning of other business criteria, such as cost-effectiveness and innovation (Henttinen, 2018).

Framework Implementation Tieris the approach the organization has taken to identify and manage the risks. Tiers describe an organization's cyber security risk management practices defined in the Framework exhibiting the characteristics, e.g. risk and threat aware, repeatable, and adaptive. Within the Tier selection process, an organization´s current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints should be considered. The Framework Implementation Tiers are not intended to be maturity levels, but they are supposed to provide guidance in organizational interactions and coordination between cyber security risk management and operational risk management (Henttinen, 2018).

2.6.1 Comparison of Standards

The idea that information system security, has become such serious element of any organization's efforts to manage risk, is what drives the need for a well-defined, carefully documented, and quantifiable way of implementing an information system security program. Security Standards can be used as guideline or framework to develop and maintain an adequate information security management system (ISIS). Organizations in the public and private sectors depend on information technology in support their missions and business functions. Information systems can be very diverse entities ranging from high-end supercomputers to very specialized systems (Kuligowski, 2009).

According to Kristian et al. (2018), there are five main steps to compare the security standards. The first one is defining common terminologies. They are defining common terminologies, analyzing existing works, defining a conceptual model and template, application of template to standards and comparison of standards. The purpose of the common terminology is to provide fixed definitions of important terms with regard to security standards as a base line to which the terms in the individual standards can be compared. Secondly, it is analyzing existing work**.** This analysis results in a set of activities, which are often prescribed in security standards. The third step is to define a conceptual Model and template. The template contains all phases of security standards considered in the conceptual model, as well as a description on how these phases have to be instantiated for a

particular standard. Next to definition of conceptual Model and template, the fourth stage is to Apply Template to Standards**.** In this phase, the templates for well-known security standards such as Common Criteria like ISO 27001 and others. The last step is to compare Standards via comparing the different instantiations of templates. In addition, which of the common terms are considered by the standards and which are not. These insights shall provide a basis for the evaluation of a particular standard.

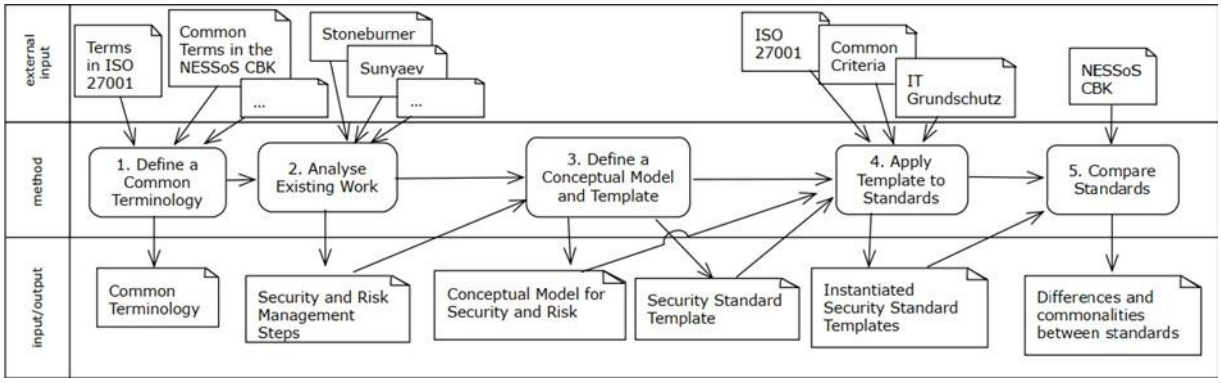

Figure3: Method for Comparing Security standards (CAST) Source Kristian et al., (2018)

2.6.2ISO (International Organization for Standardization)

The ISO 27000 series is a CSF published by the International Organization for Standardization. It is the gold standard for information security frameworks, and many others are based on its specifications (ISO, 2005). It in fact encompasses information security standards published jointly by international organizations for standardization (ISO)

One notable feature of ISO is its sheer breadth. It has 46 modules, some focusing on specific facets of information security like network security and application security, and some focusing on specific industries like health care. Whatever your customer needs, you are likely to find a module addressing it, and you can skip over unneeded areas without sacrificing effectiveness. Many organizations focus mostly on ISO 27001, which deals with threat and vulnerability assessments, developing a system customized for your organization, and recommending numerous controls in areas like cryptography, access management, physical and environmental security, and information system incident management (ISO, 2013).

ISO does not offer and does not require certification. However, many third-party organizations do offer ISO certification. The ISO series itself is not free, and certification

will add more expense. Overall, ISO encourages organizations to develop an ISSM that is right for them, treating the ISO 27000 series as a guide, not exact rules (Solar Winds, 2019).

Ejerssa, (2018) states, the ISO/IEC 27001 ISMS standard adopts the well-known PDCA process approach. The PDCA approach is also called a continuous improvement since the management system is regularly monitored and reviewed to check whether the controls to manage the risks are still effective and if they are not, then improved controls need to be implemented.

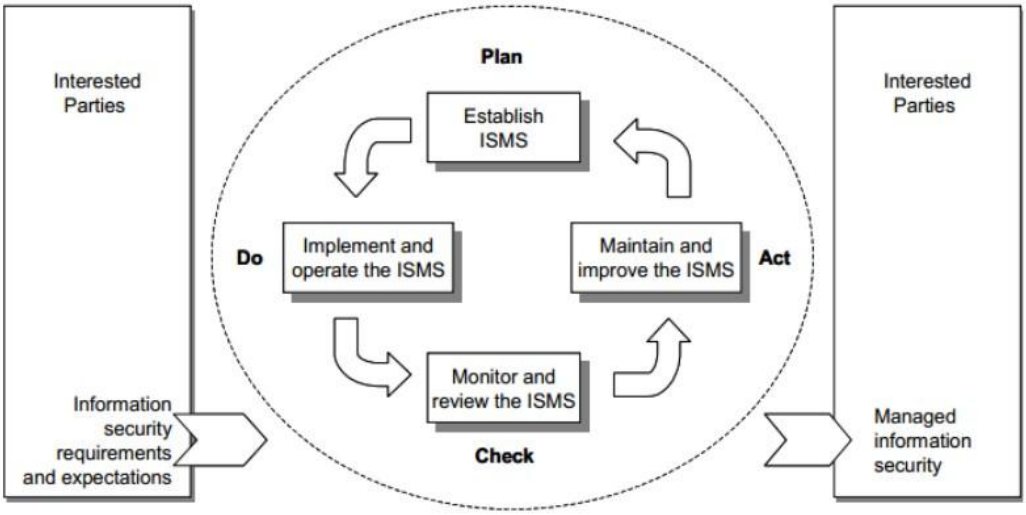

Figure 4: PDCA model applied to ISMS processes Source: ISO/IEC 27001, 2005

A massive change to the eco system which organizations are developed, for the need of a review of the old ISO/IEC 27001:2005 to the new ISO/IEC 27001: 2013. Despite, the fact the general changes are that the new standard places more emphasis on measuring and evaluating how well an organization's ISSM is performing.

The 2013 edition, with some minor differences are made to the standard itself. Some controls have changed and some merged together and terms and definitions part is deplored in 2013 edition. Additionally, ISO 27001 editions of Terms and Definitions refer to ISO/IEC 27000 standard. The most important change in standard is there is no need for PDC A model any more as continual improvement occurs. Also, there is a shift to move support of the ISMS to the executive management level. Plan: the definition of policies, objectives, targets, controls, processes, and procedures, as well as performing the risk management, which support the delivery of information security aligned with the organization's core business (Gebrhiowt, 2018). A close-fitting relation with PDCA model in 2005 edition is no longer exists. But this

does not mean that a PDCA cycle does not exist or cannot be used. Sections in 2013 edition can be harmonized with PDCA cycle (Gebrehiowt, 2018).

2.6.3 NIST SP800-53

The National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce, first published its Special Publication 800-53 in 1990 in order to help nonmilitary federal agencies adapt to Federal Information Processing Standards (FIPS). This framework contains a number of best practices for information security in government, and due to the guide's comprehensive and flexible nature, it has become extremely popular in the private sector as well (SolarWinds,2019).

The advantages of NIST 800-53 are more comprehensive than ISO 27000. Any non-governmental entities who want to work on government contracts maybe required to be certified in these best practices as well as all needed documents are available free through government websites. However, that comprehensiveness could also be a disadvantage. At nearly 500 pages, NIST 800-53 could overwhelm even experienced IT professionals, and make it an unwieldy tool for good information security management (Ibid).

2.6.4 NIST Cyber security Framework

A relative new comer from the same agency as SP800-53, the CSF was created in 2014 and published publicly several years later as the result of a US federal executive order to better protect critical infrastructure from cyber-attacks. To this end, the CSF provides a brief and accessible high-order guide to information security, cracked down into five categories: identity, protect, detect, respond, and recover (Michael et al., 2017).

While the CSF is not a truly comprehensive security framework, it is a solid foundation for small organizations that cannot afford the time or investment of ISO or NIST 800-53. It could also be effective as an introduction for non-technical executives who are responsible for information security decisions (Solar Winds, 2019).

2.6.5 Information Technology Infrastructure Library (ITIL),

The IT Infrastructure Library (ITIL) is a collection of several books on the subject of IT service management. These were developed by the United Kingdom's Office of Government Commerce (OGC).ITIL concerns the management of IT services from the point of view of the IT service provider. The IT service provider could be an internal IT department as well as an external service provider. The overall goal is to optimize and improve the quality and cost-effectiveness of IT services BSI (2008k2) (Muhametet al, 2018).

ITIL describes the best practices approaches in IT service Management, starting from strategy generation to the continual service improvements. ITIL was published in the 1980s, by the Central Computer Telecommunications Agency (now Office of Government Commerce). The first version of ITIL has 31 associated books covering all aspect of IT services (Muhametetal, 2018).

In the year 2000, was published the second version of ITIL as a set of revised books that become universally accepted for effective IT service provision and in2007,ITILV2 was enhanced and consolidated to the third version of ITIL which covers IT service lifecycle. The current version of ITIL (ITILV3) introduces framework for IT Service Management lifecycle and highlights outcomes that must be achieved to successfully implement and manage IT services. ITIL V3 is a library that contains a sets of five books and 26 different processes inside different phase so fits lifecycle that describes the processes that need to be implemented in an organization and provides a systematic approach in the area of IT Governance, management, operations and control of IT services (Muhametet al,2018).

Each of the five ITIL books gives the best practices for providing IT services efficiently and effectively. ITIL V3 framework contains five phases: They are Service Strategy; Service Design; Service Transition; Service Operation; Continual Service Improvement (Muhametetal, 2018).

ITIL V3 framework contains five phases that shows in the figure below

.

Figure 5: ITIL Framework (Muhamet, et al., 2018)

This phase can help IT planning in five key processes: Strategy Management for IT Services, Service Portfolio Management, Business Relationship Management, Financial Management, and Demand Management .It helps to identify the IT services that are needed by the organizations to understand how these services should be delivered, to define the customers, develop the offer, identify strategic assets, quantifying the value of service, financial forecast for the services and to analyze how changes in the business environment would affect the IT services (Muhamet, et al., 2018).

The service design phase includes eight processes: Design Coordination, Service Catalogue Management, Service Level Management, Supplier Management, IT Service Continuity Management, Information Security Management, Availability Management, and Capacity Management. Service design phase ensures that all IT units can deliver quality services, meet all the enterprise requirements by the alignment of IT and business needs, improve IT Governance, improve quality of service, improve consistency between IT units, and easier implementation of new services (ItSMF, 2011).

Further, there are five key aspects of service design: They are :Design of each IT services offered; Design of the services management system tools; Design of IT architectures and management systems; Design of processes needed to install, operate and improve IT services and processes; Design of measurement methods and metrics (Moeller,2013).

Service Transition phase helps to control and manage the risk of IT service failure by using contingency plans to manage the risk when new services are transitioned to a new operation level of service. It ensures that all changes comply with institution requirements to improve the consistency and quality of new service implementation ItSMF, (2011). This phase includes seven processes: Change Management, Release and Deployment Management, Service Validation and Testing, Change Evaluation, Service Asset and Configuration Management, Knowledge Management and Transition Planning and Support. According to Moeller, this phase helps in utilized standardized methods and procedures to ensure safe change management and to minimize the impact of changes in service delivery quality (Moeller, 2013).

The service operation phase contributes to perform the day-to-day operation of the processes that manage IT services. This can be achieved by the application of five processes: Event Management, Incident Management, Problem Management, and Request Fulfillment. It is also where performance indicators for the services are gathered and reported, and value is realized ItSMF, (2011). Moeller divided this phase into these categories: Service Operation Event and Incident Management and Service Operation Problem Management.

Continual service improvement phase is responsible to identify and evaluate institution needs and implement improvements to IT services to support institutional goals ItSMF,(2011).This phase helps to improve the process efficiency and effectiveness by these activities' lifecycle: Service Strategy, Service Design, and Service Transition and Service Operation. ITIL helps companies in organizing the IT service activities inside the organization to improve the quality of IT services delivered from a business and customer perspective (ItSMF, 2011).

According to Moeller, ITIL is a framework designed to support IT functions and outlines the best practices that are crucial for IT Governance, starting from checklists, tasks, procedures, and responsibilities (Moeller, 2013). He identified some of the advantages of ITIL framework application: Increased user and customer satisfaction with the IT services provided; Improved service availability, directly leading to potentially increased business profits and revenue;

Financial savings from reduced rework, lost time, improved resource management and usage; Improved time to market for the IT aspects of new products and services; improved decision-making and optimized risk for all IT related processes.

2.6.6 Payment Card Industry Data Security Standard (PCIDSS)

By some measures, PCI DSS is the most common information security framework in the world. However, it is not a framework, as its scope is too limited and its best practices do not comprehensively cover an organization's whole operations. However, it merits mention here as PCI DSS play such a big role in the information security space and it could certainly provide useful controls for MSPs building their own custom information security framework (SolarWinds, 2019).

PCI DSS was created by the five major credit card companies (Visa, Master card, American Express, Discover, and JCB) to combat credit card fraud. The first version was released in2004. It features 12 requirements in six “control groups,” which are: Build and Maintain a Secure Network and Systems; Protect Cardholder Data ; Maintain a Vulnerability Management Program; Implement Strong Access Control Measures; Regularly Monitor and Test Networks ;Maintain an Information Security Policy Compliance with PCI DSS is not government-mandated but is required by the credit card companies for every single enterprise that processes credit or debit card transactions and/or data, regardless of size or volume. The card companies levy monetary penalties for noncompliance. If your organization stores or processes card data, PCI DSS must be part of your security framework. And if you deal with any sensitive data, this is a good starting place (Solar Winds, 2019).

2.6.7 Health Information Trust Alliance (HITRUST) CSF

HITRUST (2014) asserts that after HIPAA was passed in 1996, the health care industry struggled with the law’s vague regulations and loopholes. Organizations were allowed to self- assess their cyber security threat levels, even though many hospitals and doctors' offices did not have qualified experts on staff.

HITRUST's CSF was created in 2007 to give healthcare organizations clear, actionable procedures for information security. It was made with HIPAA compliance and the healthcare industry in concentration but it is available for all organizations in all industries. It is especially useful for any industry that deals with the regulation and private data. Like other newer CSFs, it builds on the most common existing ones, with the claim that it unites and draws on elements of ISO, NIST, PCI, HIPAA, and state laws HITRUST, (2014). HITRUST

is risk-based, which means it is customizable and adaptable to your customers' threat levels. It is free for qualified organizations and certification is available, so you do not have to go it alone.

2.6.8 Control Objectives for Information and related Technology (COBIT)

COBIT is to the financial industry as HITRUST is to the health care industry. Created by the Information Systems Audit and Control Association (IASCA), the controls and best practices were defined in the1990s for financial auditors but were quickly expanded for all industries. Like HITRUST, COBIT helps with compliance for specific regulations, specifically the Sarbanes-Oxley Act.

COBIT Version 5 is the current version of COBIT and the complete package consists of: Executive Summary, Governance and Control Framework, Control Objectives, Management Guidelines, Implementation Guide, IT Assurance Guide (ISACA,1996) .COBIT is a high-level system that integrates the overlapping elements of major CSFs. It divides the IT process into four domains: Plan and Organizes, Acquire and Implement, Deliver and Support, and Monitor and Evaluate (Solar Winds, 2019).

It presents an international and generally accepted IT control framework enabling organizations to implement an IT governance structure throughout the enterprise Control Objectives for Information and related Technology is a framework for the governance and management of information and technology, aimed at the whole enterprise (Heruetal.,2011). Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. COBIT describes a method for controlling the risks arising from the use of IT to support business-related processes. In other words, enterprise I&T is not limited to the IT department of an organization but certainly includes it (ISACA, 2019).

COBIT2019 includes 40 governance and management objectives, organized in to five domains as follows; Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor Evaluate and Assess (MEA).

2.7 Information Security Management System Frameworks

An information security management system (ISMS) is a systematic approach to managing sensitive company information so that is remaining secure. ISMS encompass people, processes and IT systems. It also ensures the safety and reliability of the information, and to

enhance the organizations information security level of managerial, technical, and physical safeguards. The primary purpose of ISMS is concerned with the way, process or method in which information security is managed from the organizational perspective (Azah & Norizan, 2010). Of the many reasons to use information system security now a days are protecting organizational integrity, improving efficiency, keeping the organization information system secure and many more.

According to Suganthy and Moinak (2014), Organizational need and policies: Future concerns seems to be handling the volumes of data; hence, it is not necessary to make all the data to be secured but to secure only the data, which are important for the organizations. Identifying the critical data is also a major issue. And it is observed that the failure of the information system security is due to them is match of the organizational policy and information security policy. One of the important factors to be considered while developing an information security policy is to match the organizational policy with that of the security goals.

Threats, Vulnerabilities, and Risk: Reducing the vulnerability of the system will, in turn, reduce the chances of attacks on the system; in turn will provide tight information security. Identification of the risk and finding a mitigation plan will help to improve information security to a greater extent.

Legal Ethics: Apart from building all the protection mechanisms, it is necessary to train the user of the system to utilize the resources properly. Legal and ethical concerns should be taught to the user in all the levels of the organization.

Security Goals: The major security goals of the system include confidentiality, integrity, and availability. Every security mechanism should have a balance of all these three goals to meet the organizational requirements.

2.8. Information Security Risk in Public Sector

Risk is the possibility of something contrary happening. The process of risk management is to identify those risks, assess the probability of their occurrence, and then taking steps to reduce the risk to an acceptable level. All risk analysis processes use the same methodology. Determine the asset to be reviewed. Identify the risk, issues, threats, or vulnerabilities. Assess the probability of the risk occurring and the impact to the asset or the organization should the risk be realized. Then identify controls that would bring the impact to an acceptable level (Peltier, 2005).

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the organization's missions/business functions (NIST,2011).

Risk management is a complete process that requires organizations to frame risk, which create the context for risk-based decisions, assess risk, respond to risk once determined; and monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a complete, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision-making is integrated in to every aspect of the organization (NIST, 2011).

2.9 Information security management in the Public Sector

Nowadays government digital agendas around the world are a hot issue. For the last few decades, the business nature of public organizations is changed into a digital manner. Every corner of the organizations needs to have digitalization and produced lots of valuable information that helps to sustain the organization. Most of the Ethiopian public sectors don't have any information system security management framework as per the different surveys conducted. Different basic factors enforce to have an ISSM implementation in public sectors.

According to Veiga & Eloff, (2007). Concerning internal requirements, assert that IT infrastructure issues connected with information security help to describe requirements to secure the crucial infrastructure that constitute the information backbone. Business information issues connected with information security help to define those requirements that are relevant in terms of protecting the confidentiality, integrity, and availability of sensitive business information assets. Along with this significant expansion in digitalization, the need for implementing a Security Management System has had an increase as well. This significant increase is based on the fact that public organizations are prioritized to protect the number of outages. Thus, these companies have requirements which include be in gstrict and legal, in terms of their information security management.

2.10 Related works

Table 2 Related Works

There were numerous kinds of studies conducted in the by different scholars.

Author(year)	Objectives	Methods/approach	Keyfinding	Recommendation
Gebrehiwot, (2018)	To assess thecurrent ISM practices ofEthio telecom.	CaseStudy	No risk assessments performed by the company. Role Change is neededfrom ITdivision.	Proposed a Framework
Negussie, (2015)	To assess information security and ISP practices, and to identify the challenges and prospects of Informations ecurity policy in the Ethiopian banking industry.	explanatory	There is no such common Information security governance standard with in the banking industry of Ethiopia.	Management Support, user training, Security awareness personnel are needed, security awareness programs basically should start the begging when employee joins the organization.
Ayalew, (2016)	To assess the role of Information security culture atthe development bank of Ethiopia towards the protection of information assets of the bank ingeneral.	Case S tudy	the overall information security culture of the Bank is not conducive forthe protection of information assets.	➢ The Bank should implementa comprehensive and adequate set of information security components. ➢ The Bankshould compile a ndimplement a formalwell-defined informationsecurity policy andits derivatives ➢ the Bank should organize the information security department at ahigher
Kelemie (2013)	To propose and develop ISM Framework which will work in the banking industry in Ethiopia	Case Study	No formal and compressive developed ISMS in their bank.	Developed information security management framework for the bank

Nakrem,(2007)	Managing information securityin organizations A CASEstudy	CaseStudy	Complication of the standards	Propose Aframework of information security handling
Ejerssa, (2018)	To assess thecurrent maturity levelof information security implementation in Ethiopian public universities.	Mixed-Method	The 1st Generation universities scored better maturity scores relatively comparing to other two Higher Education Institutes generation, the third-generation universities found to be at the bottom.	Information security emphasized that management's attention is required tosecure information resources to design effective security policies, and to enhance users' security awareness of information security policies.
S.Afawaze,2011	To identify the present and discuss the information security management practice and cultural factors that may affect the implementation and development of information security	Case study	Management commitment, IT structure, Skill development and training and lack of awareness, Motivation and knowledge sharing.	Comprehensive conceptual analytical framework.

.

Mekonenn,(2 016)	to investigate the perceived importance and maturity of IT Governance practices in the financial sector of Ethiopia in terms of IT Governance Structure.	Comparative Study	The actual IT Governance practice was still Conducted on an informal and ad hoc basis with little or no evidence of standardization.	➢ IT Governance Structure. ➢ Standardization and institutionalization f IT Governance processes. ➢ Communication and collaboration between stakeholders (IT Governance relational mechanism) ➢ Policy implications
Eskatenafe and Tebebe ,(2017)	to assess the existing information security maturity level in the banking Industry in Ethiopia.	Mixed Method	there is no bank that passes the industry average information security level	Information security standards and best practices can be the best solution for effective information security management
Tsedale, (2018)	to assess the current practice of information security incident management at bank x of Ethiopia using international standard.	Qualitative and exploratory	Bank x doesn't have a separate information security incident management policy and plan	Management Support, Incident Management Policies, Awareness training,
(Lloyd, 2012).	The aim of this research was to assess information security management Chancel or College	Qualitative	Policy issues, academic freedom, Organization culture, user awareness, staffing, top management support, ICT infrastructure are the same challenges that Chancellor	➢ User Awareness ➢ Organizational culture ➢ Staffing

The views of different researchers in the information security management by using different research methods are compiled in the above table. The researcher trying to summarize in the following:

Three of the researchers use mixed method research methodology and they try to assess the Information system security in the bank industry and in the public university. They conclude that in the banking industry Information security standards and best practices can be the best solution for Information security management; and in the public universities management's attention is required to secure information resources to design effective security policies, and to enhance users' security awareness of information security policies.

By using case study, four researchers are trying to conclude for different business nature organizations. In these cases, study three of them are proposed a framework for three different organizations and the reset gives the following recommendation, implement a comprehensive and adequate set of information security components, compile and implement a formal well-defined information security policy and its derivatives, and organize the information security department at a higher possible level.

Management Support, Incident Management Policies, Awareness training, user training, Security awareness personnel, security awareness programs basically should start at the beginning when an employee joins the organization and other issues are recommended by the other two researchers and they are u s i n g exploratory and explanatory research methods.

Chapter Summary

The idea related to information system security management practices, has been discussed exhaustively in this chapter. International standards to assess the gaps of Information system security management practice also presented.

It is visible that, many literatures focus on the issues of assessing the gaps in ISSM practice. Different standards and guidelines for assessing gaps of information system security management practice are presented.

ISO is the most power full standard uses by different organizations and advised by international academicians. The researchers in many literatures applied ISO standard to assess gaps in the current practice of information system security management of different organizations.

CHAPTER 3: RESEARCH DESIGN ANDMETHODOLOGY

3.1 Introduction

The main goal of this chapter is, to give a clear picture about the research approaches, selecting the proper research methodology, and answering the research question. In this chapter, the research design and methodology for the selection of the research, type of research approach (Case study), data collection methods and data analysis techniques are described. Attend of this chapter validity and reliability of the work is discussed.

3.2 Research design

Approach of the study

A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose (Kothari, 2004).The design and methodology of a research is determined by the purpose of the research. This study explores and evaluates the ISSM of the four public organizations of Ethiopia. To properly address the research problem, the study has employed the qualitative research approach. According to Creswell (2003), research method is the choice of research approach whether it is qualitative, quantitative or mixed based on the nature of the study. To get the necessary data for the study qualitative methods were employed. Therefore in this study, a qualitative and case studies was used to collect the data and used to confirm findings from different data sources though triangulated data instrument and consequently to draw valid general conclusions. This is because qualitative approach is important to collect a wide range of data from multiple sources, and provide an interpretive and holistic understanding of the issue under study, both being relevant for a research of this kind (Cresswell, 2007)

In addition, the case study enables a researcher to closely examine the data within a specific context. In most cases, a case study method selects a small geographical area or a very limited number of individuals as the subjects of study. Case studies, in their true essence, explore and investigate contemporary real-life phenomena through detailed contextual analysis of a limited number of events or conditions, and their relationships (Zaidah, 2007). The proposed research strategy is a case study.

3.3 Methods of Data Collection

3.3.1 Data gathering Methods

Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes (Kabir, 2016). In this research, both primary and secondary data are used. For primary data collection, the researcher used Interviews.

The study used multiple sources of data. For collection of primary data, the methods employed in this study were key informant interviewing .Key informant are from among federal Ministry of Innovation and Technology (MINT) , Ministry of Science and Technology, Ministry of Finance and Economic Development (MOFED) were interviewed. Most of the key informant interviews were held before and whereas at the same time with evaluating documents both printed and electronic (computer-based and Internet-transmitted) materials. The interview was conducted with the purpose of identifying the major areas where the gaps occur. The interview method of collecting data involves a presentation of oral-verbal stimuli and reply in terms of oral-verbal responses (Kothari, 2004). A structured interview is conducted during the interview time. In group interviews or discussions, an open-ended interview is conducted.

In-depth interviews with officials' Key persons in the IT divisions, Information security heads.IT and Information system managers, Network and infrastructure managers and project managers and IT governance were conducted by purposive sampling. Purposive sampling was used in order to identify key informants In order to identify key participants within the information system division purposive sampling technique is followed, which is highly recommended for qualitative case study research (Neuman, 2003).Further in order to address the research problem ,numerous levels of data sampling were used. At MOFED and other staffs different levels. These were also purposely selected. This is because, information system division manages all the information systems functionalities including its security while the security experts or system administrators make sure that the systems are functioning as per the required policy, procedures.

The secondary data corroborate the primary data in order to support and bring evidences. Secondary data were gathered from different reports, plans, and implementations, books,

journal articles, published and unpublished documents, through qualitative documentary analysis. IT and ISSM based documents of the public organizations are reviewed. Policies, rules, regulations, and procedures based on ISSM which is implemented for the day to day activities to protect the organizational information from external and internal threat is reviewed. The document analysis was also made for cross-checking the validity of the response given on the questionnaires and interview.

Document Analysis and Observation

Observation was also used one of the source data generated .As a result the student researcher has observed working environment and the business transaction in the organizations while data collecting. The researcher prepared the checklist for observation. This checklist includes the necessary criteria that are help to observe.

Document analysis is a systematic procedure for reviewing or evaluating documents both printed and electronic (computer-based and Internet-transmitted) material. Like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted to elicit meaning, gain understanding, and develop empirical knowledge (Bowen, 2009). IT and ISSM based documents of the public organizations, policies, rules, regulations, and procedures based on ISSM which is implemented for the day to day activities to protect the organizational information from external and internal threat is reviewed. The document analysis was also made for cross-checking the validity of the response given on the interviews.

3.4 Main steps during this study

1. Literature and related work review and to release ISSM concepts.
2. Understanding the current ISSM practice in the public organizations.
3. Analyzing the collected data.
4. Discussing the findings that result in the form of data analysis with respect to the research questions.
5. Preparing the findings to propose the framework.
6. Identify the critical and mandatory requirement to propose the framework.
7. Evaluating the requirements by experts.

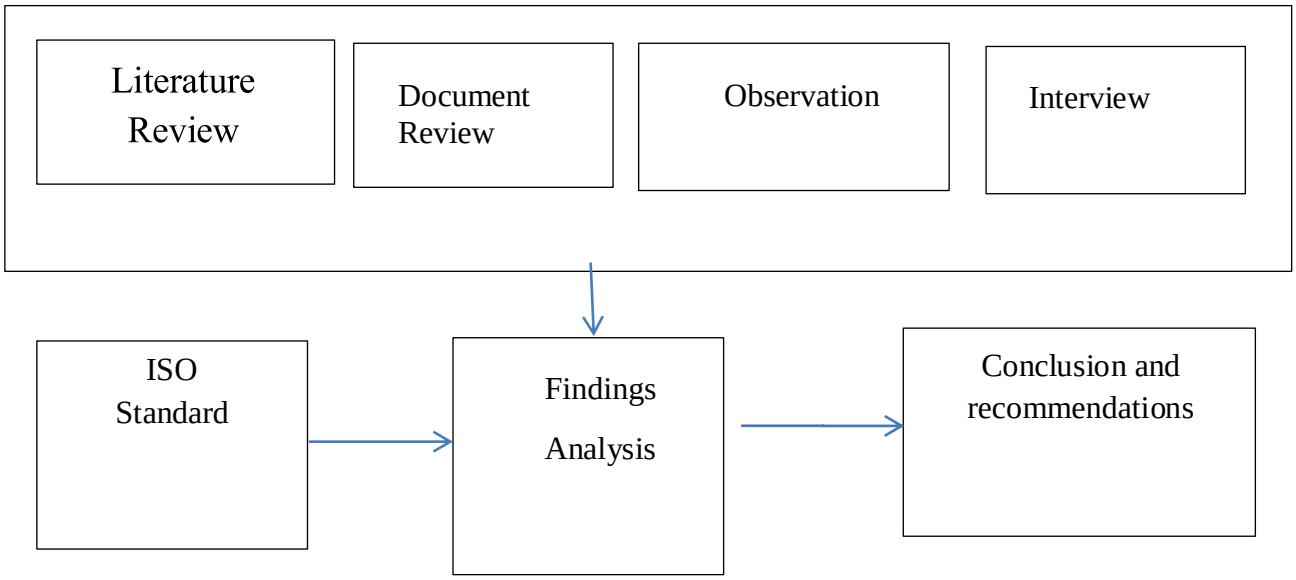

Figure 6. Research Steps

3.5 Case selection

In this research there are four cases chosen by the researcher. The main criteria to choose the cases are the business nature of the public organizations, and the four organizations are linked directly or indirectly with the other ministries. Therefore, assessing the gap of ISSM for the four organizations can help to understand the situation in the other organizations.

The culture of Ethiopian public sector organizations shows that almost all information technology tasks are done by the IT division including ISSM. In this research, the study population is the information communication technology divisions of MOFED, MOR, TECHIN, and ESSTI are incorporated. The sample selection was dependent on the size of each organization. And the users of the IS system in each organization.

3.6. Case study research method

To refer to a work as a ”case study ” may mean it is a method of evidence gathering or a real life context(George and Bernent,2005) employs a multiple sources of evidence (Yin, 2003)or the researcher investigates the properties of single phenomenon, instance or example. In addition, it employs triangulation or it relies on multiple sources of evidence and benefits from the prior development of theoretical propositions to guide data collection and analysis (George and Bernet, 2005).

Case studies are well suited for development of detailed, intensive knowledge about a single case, or of a small number of related cases moreover it focuses in contemporary events and itis applicable to real world organizations (Yin,2009).To answer the research question and

the objectives of the research case study method are suitable or this research. Zainal, (2007) clarifies that, case study method enables a researcher to closely examine the data with in a specific context. In most cases, a case study method selects a small geographical area or a very limited number of individuals as the subjects of study. Yin (1984)

The research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically (Kothari, 2004).This study identifies the current implementation of ISSM in the four public sectors, and proposing a framework to be used by the public organizations.

3.7 Sampling Methods and Techniques

A sample design is a definite plan for obtaining a sample from a given population. The sample design is determined before data are collected. There are many sample designs from which a researcher can choose (Kothari, 2004). A census is an attempt to gather information about every member of some group, called the population. Therefore; to collect full information, the researcher selects the census for all information technology staff. Depending on the size of the organization census might be conducted for the user side. However, if the size of the users is too large purposive sampling techniques are conducted.

The sampling method for this research is purposive sampling. According to Kothari, (2004) in this type of sampling, items for the sample are selected deliberately by the researcher; his choice concerning the items remains supreme. According to (Gebrehiwot, 2018) purposive sampling refers to a process where participants are selected because they meet criteria that have been predetermined by the researcher as relevant to addressing the research question. Hence, the source of the population was taken from the Information systems division. The respondents were chosen because of their role in IT and the functions they performed within the process areas

3.7.1 Sample scope

It refers to a list or set of direction that identifies the population. The target population of this study is the employees of the selected organizations, but if the organizations have a security division, the scope will be the member of the ISM divisions of the selected organizations.

3.8 Validity and Reliability

In any research to check the quality validity and reliability are must be applied. The following methods are used to check validate and reliability of the work.

Interview, document analysis, and observation are conducted for collecting the data of this research used, which allows the researcher to achieve the goal and to answer the research question. According to Myers (2009), triangulation of data from different sources increases the quality of data, and accordingly the accuracy of the findings.

The interview was adapted from international information security management standards of ISO/IEC 27001:2013. After the interview is adapted, modifications and adjustments were made on the formatting after discussing with the advisor. The initial drafts of each of the structured interviews reports are emailed to the respondents of each organization in order to confirm them for accuracy and to review them for comments, correction, and further feedback and clarification.

After summarizing the interviews each report are sent by email to the interviewees of the organizations in order to verify them for accuracy and to review them for comments, and further feedback and clarification if necessary.

3.9 Data Analysis

The computation of certain indices or measures along with searching for patterns of relationship that exist among the data groups is called Analysis (Kothari, 2004). After collecting and organizing the necessary data separately for each item to answer the questions raised in the problem statement. Thematic analysis for qualitative results is done.

Chapter Summary

In this chapter the methodological approaches in the IS has been presented to provide this research. The qualitative approach facilitated the researcher to associate more closely with the participants, and to identify issues of substance and interpretation that they give to their organizational activity. It is decided that multiple case study plan is the most appropriate strategy for this investigation. The data gathering methods that were employed included semi-structured interviews, observation and document analysis.

This allowed the researcher to get the appropriate thoughts, experiences, ideas, opinion sand knowledge of the participants. The qualitative thematic analysis is judged to be the appropriate technique for studying the data. Methodological validity and reliability are discussed at the end of this chapter.

CHAPTER 4: PRESENTATION AND ANALYSIS OF FINDINGS

4.1. Overview

The main target of this chapter is to rationalize and clarify the research methodology of the study. Presenting the findings from the analysis of this case study research is the other goal of this chapter. The researcher analyzes the overall image of ISSM in public organizations. It is a multiple case study, the researcher attempted to understand the ISSM based on the participant's responses to the interview questions and their experience in the ISSM and other related projects. The majority of the respondents did not want to mention their names and personal information. While some of them were interested therefore, the individual's names and personal information are kept anonymous and pseudonyms are used instead.

Positions	Pseudonyms	Number of Participants
Directors	➢ Director1 ➢ Director2	2
Security Team Leaders	➢ Team Leader1 ➢ Team Leader2 ➢ Team Leader3 ➢ Team Leader4 ➢ Team Leader5	5
Network Team Leaders	➢ Net TeamLeader1 ➢ Net TeamLeader2 ➢ Net TeamLeader3	3
Network Professionals	➢ Net-prof1 ➢ Net-prof2 ➢ Net-prof3	3
System and Application developers	➢ Sys and app1 ➢ Sys and app2 ➢ Sys and app3	3

Database Admin	➢ Database Admin1 ➢ Database Admin2	2
Other IT Professionals	➢ Other IT1 ➢ Other IT2	2

Table 3. Interviewee

4.2 Interviewee Profile

With regard to interviewee profile, the researcher interviewed team leaders, experts and tried two collect documents. The total respondents were 20 in number. Out of the total respondents the gender distribution of the respondents is, male 18 and 2 are females. Therefore the majority of the interviewee 18(90 %) were male while the 2 (10%) were female interviewee respondents. This also implies that there is much work to be done in order to balance the number of male and female IT professionals.

With respect to educational status of the interviewee, out of total participants 11 of them were first-degree holders .8 MSC and one was a PhD holder. These imply that the respondents are educated and they are able to answer the interview questions with good understanding.

4.3 Key Findings: Case Study analysis

The following sub section comprises detailed analysis and description of the case study. The analysis is compiled and developed based on the examination of the data gathered from the interviews, document analysis, and observation.

As key findings, the three proposed research questions at first chapter based on the statement of the problem were treated in this part of the study. As aforementioned earlier, the research questions were forwarded systematically to the respondents with data collection instruments like interview, document analysis and observation. The first question presented to interview participants was "What are gaps in the Information Systems Security Management practice in public sector organizations? The data collected in the interviewee reelected that there are challenges and the implementation of ISSM is not well achieved with respect to what is planned. Based on the first interview questions, Information security policies Management, the interviewees were asked to respond to describe and list the drawbacks and strength of existing approaches in information security management through the institutions and have got gaps likewise lack of skilled professionalism, low level of organization of information

security, communications security, and physical and environmental security are among the common gaps. However the system applied by the four institutions includes a number of technological and scientific supports the ISSM management highly. In addition, if effective application of ISSM in the organizations there could be application of policies, regulations in order to achieve the objective planned and expected from the organizations. Further, the observations pointed that almost all of the institutes have their own well-designed data center one of the institute data center are a part from the main office. The physical security for the data centers is very good as well as it has a biometric and pass word door lock incorporating a CCD camera.

Moreover, the fire extinguisher is also put in every corner of each institute. In the security office in two organizations, the security team has their own office but the others are sharing office with other IT stuffs. The instrument especially the network instruments are physically secured, switches, and access points are wall-mounted with appropriate rack. To the contrary, there were challenges observed in the facilities of the organizations. The working environment of one organization out of four is not suitable for the employees. Four instance, Key informant explains that the non-suitability of the working environment was because of the new structure they are on the process to change the office. And the new structure is underway to be in a new office.

Since information is growing faster than any time in history, its management and need to safeguard it and mange it efficiently and effectively is very useful. As Betrand,(2002) asserts that different organizations like corporations from small to big, whether they are public or private need to safeguard and secure their information. Besides, ISSM policy helps to facilitate the information security with in each organization. In relation with this, the key informants were presented with question of whether information system security policy is applied in their organizations. The respondents were asked to answer whether their institutions have Information Management Security Policy to establish secured information management in line with the objective of the organizations. In response it is found out of five security professionals from four public organizations replay that:

> "There is no independent standard security framework or policy in the organizations, rather the reins an obsolete and none reviewed IT policy,whichincorporateinformationsecurityasasubtitleandwhichisno tenoughforISSM."(Key informant interview, Addis Ababa Ethiopia)

And also from the discussion it was found out, the majority of IT staffs and other staffs didn't know about the existence of the IT policy as well as there is no stated means to manage

information and information security situation with added lack of gap of knowledge of recognition of ISSM. In some organizations previously, the policy was trying to implement, but there was great resistance from the staffs. The awareness level about ISSM is also very week." Hence, it is recommended further to create awareness and training on the issue at hand.

As a result describing efforts on going to asset and modify the challenge of ISSM awareness creation **Key Informant** (**Team Leader 2)** replied that in the active directory there are some ongoing efforts to use our configuration very well and it seems like a regular security policy." As ISMS is an instrument that embraces that the management should use to clearly mange plan, adopt, implement, supervise and improve the task and activities aimed at achieving information security. The BSI standard 100(2008) elucidates that information security process policy for information security in which the information security objectives and strategies for their implementation are needed to be documented. With regards to this Key Informant **(Team Leader 3)** replies "that there is a newly established team which develops the information technology policy and especially a security framework within a year."

Appreciating this effort, the team is expected to reference all the necessary required areas of information security governance and include the use of an appropriate mix of policies, standards, guidelines, codes of practices, technical controls. Because when there isno Information security policy or framework, in a given organization with aforesaid mechanisms or instruments and it is not regularly reviewed with further absence of ISSM allows the organizations to be attacked easily. In previous time, the security issue was not getting attention and as a result every security issue passes through INSA.
Besides identifying the existence of ISSM, the IT policy and framework application practices in the four institutions were assessed. Key Informant (**Director1and2)** replied that:

> "These organizations have an IT policy which is published in 2009 E.C but it is not regularly reviewed. Due to some reason, there is current implementation and communication with the Stuffs. In the next fiscal year, organizations have a plan to fully implement."(Key informant,)

Regarding, the management role Director1adds the following*:*

> "The top-level management has a controlling and supporting the information system security as a whole and creating collaboration with in different national and international stakeholders. The directors have a role in controlling the implementation and creating awareness for all status reporting the major issues for the high-level managers."

Here again key informant (director ,2) admits that absence of dedicated absence of management, security professions and controls In addition the **Key informant (director 2)** stated that the IT policy and framework in the institution was published in 2004 E.C (1998) and includes the necessary framework and policies, codes, and other related to IT including security. However, it is too limited and narrow. In addition, it is not timely and frequently reviewed and communicated with the staff in detail. Following this, the directorate is planning to have a project in collaboration with INSA therefore, it could support and gives a chance to review and fully implement a strong IT policy (Ibid). From this interviewee result, it can be summoned that the organizations need to further strengthen and there is gap in real commitment towards employing ISSM.

In addition, **Key informant (Director 2)** comments about the management role and states a state minister controls IT division. The state minister supports every action frequently, but he states that there is problem that emanates from need and goal difference. Based on the newly established minister and these directorates have got incompliance in demand towards the necessity of IT in the business continuity. He also further assert that before a year and half ago, the organization had debated on the underpinning of organizing information security and IT professionals and latter it was allowed to establish security team. As a result, the directorates IT division and support made to them in any of their needs, especially security-wise cyber security is a new phenomenon for the country therefore it is highly supported security team with additional support of training and other issues that they need.

In line with discussions made with above the professional training is the most challenging issue is skilled professionalism. ICT professionals are people which directly involved with information security management relating tasks in the organizations as mentioned in the previous sections. Organizations are challenged with lack of skilled challenges. Besides, in most institutions in order are mile- high level cyber security professionals are responsible for

protecting IT infrastructure, edge services, networks and data. More granularly, IT professionals are responsible for preventing data breaches and monitoring and reacting to attacks. **Key Informant (Team leader One)** stated that skilled individuals are the main problems in the field of security these institute. The IT professionals become go-to resource for colleagues and can raise their profile within their organizations. The IT skilled Professionals shortage continues to be the root causes of increasing security incidents and rising security shortage. As a result, there are gaps, enforcing to ask INSA directly. Hence, starting from last year, INSA tries to give us training about information security but it does not give us a chance to directly involve in some security issues which means the training is not enough. In the organizations, there are issues like responsibility for the protection of individual assets, and for carrying out specific security processes.

The greatest benefit of security culture is the effect it has on other dynamic interconnections within an organization. The duties and responsibilities of security staffs are various kinds. Besides the duties and responsibilities of the security staffs, documented procedure all projects that go through in information security assessment. Mobile device, removable media and personal email usage policy are incorporated.

Regarding the individual responsibility, all the team leaders stated that. There is no responsibility for individual asset. However, it is everyone's responsibility and there is no well-documented procedure in any policy or written document wise." In the today's world where the information security is treated is growing rapidly in size and sophistication. However, all have forwarded to include new security policy in the future. Team leader 1 and 2 stated that, because of a lack of skilled professionals and the team age there are no duties and responsibilities separation According to Key informant (**Team leader 3 and 4)** stated that, there are no skilled professionals on the field but there is a responsibility shared between the stuffs in the team. While Key informant (**Team leader 1) says that**, all the IT projects are pass through INSA security team that works together with us. And Key informant **Team leader 2,3,4** stated that, there is no such a security check procedure in their organization but after the implementation if something is happening, they need the security assessment. In all institutes, there are no cryptography, mobile and other individual's media policy or usage procedure.

4.3.1 **Practice of Physical and environmental security**

Physical and environmental security incorporates the following ideas physical security perimeter, physical protection measures, environmental hazards identification, UPS system,

or backup generator. From the observation made, there is a security perimeter in all organizations, but it is not well defined and documented. Subsequently there is no proper protection measure, but there are things like CCD cameras and other things to prevent natural disasters. For malicious attacks or accidents, they use a firewall and antivirus in common. They are trying to identify an environmental hazard in every time, and there is a disaster recovery system that is not convenient and it is now reconstructed in all organizations. Key informant (**Team leader 1 and 2) state that** they have a well-designed UPS system and generator as well, and it is tested regularly.

4.3.2 Practice of Communication Security

Communication security focuses on confidentiality, integrity and availability of data in motion .Further; it asks the question what are the procedures for how data should be transferred made available to all employees, relevant technical controls in place to prevent non-authorized forms of data transfer? In line with this the security in the information communication Teamleader1 says that, It is very difficult to get data, there are no rules or procedures may be in the future at the end of the new project there are some rules or procedures." And **Teamleader2**says"Getting data from our organization is very difficult there are no rules or procedures, but if the ministers or the state ministers orders for some special issue you can get it." **Team leader 3 and 4** stated that, "there is no Data transfer policy but in the traditional method there are some procedures for information transfer but it are not documented." I t could be interpreted that the communication security is very tight and strong in its nature.

4.3.3 Practice of Risk assessment

Broadly speaking, a risk assessment is the combined effort of identifying and analyzing potential events that may negatively impact individuals, assets, and/or the environment. Key informant **(Teamleader1, 2, 3)** confirmed that, in this fiscal year there is a process a risk assessment on three different levels. High, Medium, and low levels and engagement to analyses the results, it shows that it must be a risk assessment not annually." Risk assessment is made which helps to identify hazards and risk factors that have potential to cause harm. In addition, **Team leader 4** says that, there is a risk assessment plan and implemented based on the plan that is flexible when there is need arousals. Risk assessment is one of the main duties that are done in the security team at all levels. All the selected organizations have done the risk assessment but they do not have any regular time and plan for the task.

4.3.4 Practice of Information security incident management

Information security incident management is the other main issues that the ISSM must incorporate it. In this part, there are issues that the researcher wants to ask the respondents. Some of the issues are clearly documented and identified management responsibilities in the incident management processes, a process for reporting of identified information security weaknesses, incident response framework that allows the organization to learn from information security incidents and reduce the impact/probability of future events.

In all organizations, it is found that there are no clear and defined documentation about the management role in the information systems security incident management. Some of the managers are involved in some cases directly or indirectly. Key informant (**Teamleader3)** asserts that, there were incidents before two years ago and it is directly informed for the director and then the director informed for the state minister to solve it with cooperation or INSA personals and solved the problem with the help of INSA. "All the respondents' agree that incident management is a task after an incident has happened. Therefore, there is no timely reporting process, that helps to identify the security weakness of the organizations. And also, there is no defined framework or policy in the security incident management.

4.3.5 Practice of Access Control, Asset Management and Operation Security

The question about operational security, access control, and asset management, followed by, access to information and application, ensuring user access rights, access control policy, and interactive or complex password systems was to respondents. In relation with this, all Network Professionals and Other IT Professionals replied that," There is no such a defined process as a policy or rule; we are on the process of developing access control procedure. Therefore, after the implementations it answers every access control. Based on the active directory configurations it differs from organization to organization it can be run all the procedures that help to create access control.

Regarding asset management was not clearly understood. In all organization's assets management means only physical management like annual inventory and other related issues. The physical asset shelf life and updating the assets are not considered. Key informant (**Database Admin 1)** stated that, the staff understood and identified the inventory in both hardware and software and also database wise, and produced a check list for activity. At the end of every inventory it is reported that for the higher officials with the recommendation of some points like changing the equipment and other necessary issues. In addition, Key Informant (**DatabaseAdmin2)** states that, "it has different aspects in some cases if the official's asks or enforces us to support others we are directly involving, in some cases related to the database we are also involved directly."

The next main issue is information security aspects of business continuity management, concerning the organization's continuity plans. The respondent replies that, **Sys and app 1, Sys, and app 2 and Other IT 1** stated, "There must be an awareness creation about the organization continuity plan for all IT and none IT stuffs. The business continuity management is included in the organization's continuity plans, but the plan was not reviewed and updated, and also no one considers that is necessary for the organization business continuity as a whole. The documentation processed is answered after the deployment of the policy." Net-prof 1 adds, "The whole security-based policies and frameworks are reconstructed in collaboration with INSA. Therefore, we might have an answer for every business continuity action in our organization."

Over all it was found that, the researcher asks the directors about the general gaps in ISSM. lack of experienced human resource in the field ,unable to implement an IT system ,lack IT policy, lack of training ,lack of user side understanding Violating Rules and regulations.

4.3.6 Summary of Interview findings

Respondents	Summarized interview findings
Directors	• Lack of IS framework and Lack of skilled professionals in the area is the biggest problem in our day to day organizational activities" • Whenever new personnel comes to the position, he/she trying to implement their own rule, because there is no defined framework for ISSM.
IS security Teamleaders	• Are enforcing the management to implement a clear and well-defined ISSM framework. • The advantage of the ISSM framework must be defined • Creating the awareness. • Lack of Skilled professionals. • Lack of risk assessment program. • There is no asset management
Network TeamLeaders	• They are using AD to control the overall activities. trying to configure a high-level security in AD every time and, all the • Staffs are resisting and disobeying. • Lack or risk assessment program. • Lack of security tools.
System and Application developers	• Lack of collaboration between the security officials and the developers • Lack of risk assessment in the systems or software.

Table 4 Summary of Interview findings proving Policy and framework as a key advantage forISSM

From the summary it can be summarized as of the interview result in the above table mainly focuses on policy and framework as a key advantage for ISSM. In all interviewed organizations the respondents are explained, there is no formal and compressive developed ISSM framework or policy. Nevertheless, there is an IT policy that is not regularly reviewed and it has so many problems during implementation and the top-level management doesn't support, lack of top management understanding about ISSM, asset inventory, risk assessment, there is no security requirement identification methodology or model of security requirement identification.

4.6.3. The selected ISSM basics and their significance

This study proposes for the selected public organizations, how to protect their information systems against threats. ISO 27001:2013 is categorized as critical, mandatory and non-mandatory. Each controls are basics for ISSM management. Based on this study, out of the 114 controls 30 of them are critical, 77 of them are mandatory and 7 of them are non-mandatory by considering the public organization existing situation. The controls and clauses are summarized as follows.

REFERENCE	COMPLIANCE ASSESSMENT AREA(SECTION)	STATUS
A.5	**INFORMATION SECURITYPOLICIES**	
A.5.1	**Management Direction for Information Security**	
A.5.1.1	Policies for information security	Critical
A.5.1.2	Review of the policies for information security	Critical
A.6	**ORGANIZATION OF INFORMATIONSECURITY**	
A.6.1	**Internal Organization**	
A.6.1.1	Information security roles and responsibilities	Mandatory
A.6.1.2	Segregation of duties	Mandatory
A.6.1.3	Contact with authorities	Mandatory
A.6.1.4	Contact with special interest groups	Non-Mandatory
A.6.1.5	Information security in project management	Critical
A.6.2	**MOBILE DEVICE ANDTELEWORKING**	
A.6.2.1	Mobile device policy	Mandatory
A.6.2.2	Teleworking	Mandatory
A.7	**HUMAN RESOURCESSECURITY**	
A.7.1	**PRIOR TOEMPLOYMENT**	
A.7.1.1	Screening	Mandatory
A.7.1.2	Terms and conditions of employment	Mandatory
A.7.2	**DURINGEMPLOYMENT**	

A.7.2.1	Management responsibilities	Critical
A.7.2.2	Information security awareness, education and training	
K8 A.7.2.3	Disciplinary process	Critical
A.7.3	**TERMINATION AND CHANGE OFEMPLOYMENT**	
A.7.3.1	Termination or change of employment responsibilities	Mandatory
A.8	**ASSET MANAGEMENT**	
A.8.1	**RESPONSIBILITY FORASSETS**	
A.8.1.1	Inventory of assets	Mandatory
A.8.1.2	Ownership of assets	Mandatory
A.8.1.3	Acceptable use of assets	Mandatory
A.8.1.4	Return of assets	Mandatory
A.8.2	**INFORMATIONCLASSIFICATION**	
A.8.2.1	Classification of information	Critical
A.8.2.2	Labelling of information	Critical
A.8.2.3	Handling of assets	Mandatory
A.8.3	**MEDIAHANDLING**	
A.8.3.1	Management of removable media	Mandatory
A.8.3.2	Disposal of media	Mandatory
A.8.3.3	Physical media transfer	Mandatory
A.9	**ACCESSCONTROL**	
A.9.1	**BUSINESS REQUIREMENTS FORACCESS CONTROL**	
A.9.1.1	Access control policy	Mandatory
A.9.1.2	Access to networks and network services	Critical
A.9.2	**USER ACCESSMANAGEMENT**	
A.9.2.1	User registration ank2dde-registration	Mandatory
A.9.2.2	User access provisioning	Mandatory
A.9.2.3	Management of privileged access rights	Mandatory
A.9.2.4	Management of secret authentication information of users	Mandatory
A.9.2.5	Review of user access rights	Mandatory
A.9.2.6	Removal or adjustment of access rights	Mandatory
A.9.3	**USERRESPONSIBILITIES**	
A.9.3.1	Use of secret authentication information	Critical
A.9.4	**SYSTEM AND APPLICATION ACCESSCONTROL**	
A.9.4.1	Information access restriction	Mandatory
A.9.4.2	Secure log-on procedures	Mandatory
A.9.4.3	Password management system	Critical
A.9.4.4	Use of privileged utility programs	Mandatory
A.9.4.5	Access control to program source code	Non-mandatory
A.10	**CRYPTOGRAPHY**	
A.10.1	**CRYPTOGRAPHICCONTROLS**	
A.10.1.1	Policy on the use of cryptographic controls	Mandatory
A.10.1.2	Key management	Mandatory

A.11	**PHYSICAL AND ENVIRONMENTAL SECURITY**	
A.11.1	**SECUREAREAS**	
A.11.1.1	Physical security perimeter	Mandatory
A.11.1.2	Physical entry controls	Mandatory
A.11.1.3	Securing offices, rooms and facilities	Mandatory
A.11.1.4	Protecting against external and environmental threats	Mandatory
A.11.1.5	Working in secure areas	Mandatory
A.11.1.6	Delivery and loading areas	Non-Mandatory
A.11.2	**EQUIPMENT**	
A.11.2.1	Equipment siting and protection	Mandatory
A.11.2.2	Supporting utilities	Mandatory
A.11.2.3	Cabling security	Mandatory
A.11.2.4	Equipment maintenance	Mandatory
A.11.2.5	Removal of assets	Mandatory
A.11.2.6	Security of equipment and assets off-premises	Mandatory
A.11.2.7	Secure disposal or reuse of equipment	Mandatory
A.11.2.8	Unattended user equipment	Mandatory
A.11.2.9	Clear desk and clear screen policy	Mandatory
A.12	**OPERATIONSSECURITY**	
A.12.1	**OPERATIONAL PROCEDURESAND RESPONSIBILITIES**	
A.12.1.1	Documented operating procedures	Critical
A.12.1.2	Change management	Mandatory
A.12.1.3	Capacity management	Mandatory
A.12.1.4	Separation of development, testing and operational environments	Critical
A.12.2	**PROTECTION FROMMALWARE**	
A.12.2.1	Controls against malware	Critical
A.12.3	**BACKUP**	
A.12.3.1	Information backup	Critical
A.12.4	**LOGGING ANDMONITORING**	
A.12.4.1	Event logging	Critical
A.12.4.2	Protection of log information	Mandatory
A.12.4.3	Administrator and operator logs	Non-Mandatory
A.12.4.4	Clock synchronization	Mandatory
A.12.5	**CONTROL OF OPERATIONALSOFTWARE**	
A.12.5.1	Installation of software on operational systems	Critical
A.12.6	**TECHNICAL VULNERABILITYMANAGEMENT**	
A.12.6.1	Management of technical vulnerabilities	Mandatory
A.12.6.2	Restrictions on soft-ware installation	Mandatory
A.12.7	**INFORMATION SYSTEMSAUDIT CONSIDERATIONS**	
A.12.7.1	Information systems audit controls	Critical
A.13	**COMMUNICATIONSSECURITY**	
A.13.1	**NETWORK SECURITYMANAGEMENT**	

A.13.1.1	Network controls	Critical
A.13.1.2	Security of network services	Critical
A.13.1.3	Segregation in networks	Mandatory
A.13.2	**INFORMATIONTRANSFER**	
A.13.2.1	Information transfer policies and procedures	Critical
A.13.2.2	Agreements on information transfer	Critical
A.13.2.3	Electronic messaging	Mandatory
A.13.2.4	Confidentiality or non-disclosure agreements	Mandatory
A.14	**SYSTEM ACQUISITION, DEVELOPMENTAND MAINTENANCE**	
A.14.1	**SECURITY REQUIREMENTS OFINFORMATION SYSTEMS**	
A.14.1.1	Information security requirements analysis and specification	Critical
A.14.1.2	Securing application services on public networks	Critical
A.14.1.3	Protecting application services transactions	
A.14.2	**SECURITY IN DEVELOPMENT ANDSUPPORT PROCESSES**	
A.14.2.1	Secure development policy	Mandatory
A.14.2.2	System change control procedures	Mandatory
A.14.2.3	Technical review of applications after operating platform changes	Mandatory
A.14.2.4	Restrictions on changes to software packages	Mandatory
A.14.2.5	Secure system engineering principles	Mandatory
A.14.2.6	Secure development environment	Critical
A.14.2.7	Out sourced development	Mandatory
A.14.2.8	System security testing	Critical
A.14.2.9	System acceptance testing	Mandatory
A.14.3	**TESTDATA**	
A.14.3.1	Protection of test data	Mandatory
A.15	**SUPPLIERRELATIONSHIP**	
A.15.1	**INFORMATION SECURITY INSUPPLIER RELATIONSHIP**	
A.15.1.1	Information security policy for supplier relationships	Mandatory
A.15.1.2	Addressing security within supplier agreements	Mandatory
A.15.1.3	Information and communication technology supply chain	Mandatory
A.15.2	**SUPPLIER SERVICE DELIVERYMANAGEMENT**	
A.15.2.1	Monitoring and review of supplier services	Mandatory
A.15.2.2	Managing changes to supplier services	Mandatory
A.16	**INFORMATION SECURITYINCIDENT MANAGEMENT**	
A.16.1	**MANAGEMENT OF INFORMATIONSECURITY INCIDENTS ANDIMPROVEMENTS**	
A.16.1.1	Responsibilities and procedures	Critical

A.16.1.2	Reporting information security events	Critical
A.16.1.3	Reporting information security weaknesses	Critical
A.16.1.4	Assessment of and decision on information security events	Mandatory
A.16.1.5	Response to information security incidents	Critical
A.16.1.6	Learning from information security incidents	Mandatory
A.16.1.7	Collection of evidence	Mandatory
A.17	**INFORMATION SECURITY ASPECTSOF BUSINESS CONTINUITYMANAGEMENT**	
A.17.1	**INFORMATION SECURITYCONTINUITY**	
A.17.1.1	Planning information k2securitycontinuity	Critical
A.17.1.2	Implementing information security continuity	Mandatory
A.17.1.3	Verify, review and evaluate information security continuity	Mandatory
A.17.2	**REDUNDANCIES**	
A.17.2.1	Availability of information processing facilities	Mandatory
A.18	**COMPLAINS**	
A.18.1	**COMPLAINS WITH LEGAL &CONTRACTUAL REQUIREMENTS**	
A.18.1.1	Identification of applicable legislation and contractual requirements	Mandatory
A.18.1.2	Intellectual property rights	Mandatory
A.18.1.3	Protection of records	Mandatory
A.18.1.4	Privacy and protection of personally identifiable information	Mandatory
A.18.1.5	Regulation of cryptographic controls	Mandatory
A.18.2	**INFORMATION SECURITYREVIEWS**	
A.18.2.1	Independent review of information security	Mandatory
A.18.2.2	Compliance with security policies and standards	Mandatory
A.18.2.3	Technical compliance review	Non-Mandatory

Table 5: Critical, mandatory and non-mandatory requirements of ISSM for Public organizations in Ethiopia.

4.8. Summary

In this chapter, based on the information collected from the participants, the findings are discussed. The findings of the research are analyzed and discussed based on the ISO27001:2013 controls. The gaps of ISSM practice in the selected public organizations are identified. The next chapter will present conclusion, recommendation limitation, and future work of this research.

CHAPTER FIVE CONCLUSION AND RECOMMENDATIONS

5.1 Overview

This chapter presents the conclusion and recommendation of the study based on thefindings of the research. Finally, the chapter proposes a clue for future research and limitation ofthe research.

5.2 Conclusion

The main objective of this research was to assess the gap of *ISSM* for the selected public organizationsinEthiopia.Findingsfromtheassessmentbasedonthefact-findingtechniques employed, such as interview survey, observation and intensive literature review indicates that the current information system security management in the public organizations has lack of a formalized comprehensive framework and Information security policy. This seemed to have an adverse effect on the effective management of information security. In the selected organizations by using the international standard ISO/IEC 27001 ascertaining the gaps and classify the critical and mandatory requirements of ISSM.

A literature review has been done to clarify terms related to, Information systems, information security, Information security framework, and information security management. Using the qualitative method mainly to assess the current practice of ISSM in the selected public organizations.

Differentresearchesaredoneinthisareaforthefinancialandtelecomsectors.The business nature of the public organizations is different from these sectors.

Findings of the research show that access management records are recorded in the IT service management system. This enables the company to track changes in the roles of employees and security breaches. The other main finding of this research is, there is no ISSM independent policy or framework. It shows that the organizations needed the ISSM framework to control the overall activates of the information security in the organizations.

For this clarification, Attempts were done to examine and compare the available international standards and guidelines. ISO/IEC27001:2013 was used in assessing the current practice in the organization. Based on the gap found by the assessment the researcher identifies the critical and mandatory requirements for ISSM based on ISO/IEC270001:2013 standard for public organizations in Ethiopia to be adopted and deliver secured service in the country.

The finding of the study shows that public organizations, physical access security management seems to be in a good position. Many people in the company are confident regarding the physical security of the IT devices and systems. Access control, operations security, and business continuity aspects are also in a good position, though more improvements may be required to be considered.

Human resources, especially the technical staff, do not have awareness of emerging technologies. This will increase the vulnerability of the company to a security breach. The results show that almost no risk assessment is performed by the company. Failure to regularly conduct risk assessment of IT systems will expose the company to attacks caused by changing technologies and threats.

There is no relationship between Vendors and other equipment & systems suppliers. Risks associated with asset management of the organizations must be improved. The finding of the survey shows that, an Ethiopian public organization does not get its systems assessed by external expertise or consultancies. Third parties have the necessary tools and expertise for risk assessment in different views from the existing organizations. Public

Organizations do not also make regular risk audit or assessment by itself. This will make the organizations not able to identify the potential risks arising from business procedures.

5.3. Recommendation

The analyzed gaps used as preliminary findings and potential indicators work for public organizations in the area of ISSM in Ethiopia. It helps the organizations to manage their information system security management. The identified gaps can serve for managers to formulate policies and procedures, for developers to develop information security systems and finally to create a common ISSM platform for all Ethiopian public organizations. The results from this research also infer additional works for researchers and academicians.

Organizational Context

The initial phase of success in ISSM is to understand understands organizational context. It means taking some time to understand the kind of services that the organizations offer to customers, and understand the kind of risks in the organization. After all this, the organizations can build ISSM framework in the right path the organization business pattern and protect those processes basically from the ISSM.

Top-level management support

The top-level management commitment for implementing the ISSM framework and other security issues is the backbone of the organizations. ISO 27001:2013 emphasize a top to bottom style for the implementation of ISSM. Setting a clear strategy, budget, and creating a smooth platform is the main task that requires from the top-level management. And the management should regularly review and checked each and every day to day activates and the framework.

Planning

Planning is the other main issue in the ISSM implementation. Implementation of the ISSM can be complex due to the organization business nature and span. An extensive and clear plan must be needed including timeline responsibilities, budget, and human resources.

Scoping

Scope is the other issue in the implementation phase of ISSM. Organizations need to have a clear scope that will cover. This will include people, processes, and technology. Some organizations here in Ethiopian needs to implement based on the ISO27001implementation scopes, but the business nature does not support them. All the inclusions and exclusions

should be documented with justifications, especially if the organization is considering a certification against the standard.

Document risk assessment methodology

There are different existing risk assessment methodologies, like ISO 27005, (NIST) National Institute of Standards, (OCTAVE), Operationally Critical Threat Asset and Vulnerability Evaluation, (ENISA) European Union Agency for Network and Information Security and (FAIR) Factor Analysis of Information Risk are some of them that the organizations might adopt the appropriate one related to their business nature. The selected method may help the organization to identify the kind of risk that the organization faces. The methodology must include at least the following steps. Asset identification, risk identification, risk analysis, risk evaluation, and measurement.

If the organizations have a plan to certify in the ISO against the standard, it needs to have a documented risk register which includes asset, asset values, risk values, risk treatment, and residual risks and risk treatment measures or plans.

Statement of Applicability

The risk assessment and treatment results will provide organizations with an indication of what controls they need to manage risks to acceptable levels. The SoA document needs to provide justification for non-mandatory applicable controls, the objectives to be achieved with the controls, and a description of how they are implemented.

Define criteria to measure the effectiveness of controls

There are different criteria to measure the effectiveness of implemented controls. Developing the necessary parameters based on the need and types of ISSM is a very vital issue. Individual controls or control objectives are defined as measurement criteria. It must be included in the implementation phase of ISSM in the organizations.

Implement controls

Introducing new technologies, processes, or changes in the organization business nature can be defined as the implementation of controls. It might face a big challenge from the end-users in the organizations. To resolve the challenge from the end-users we can create awareness and regular training before and after the implementation.

Creating awareness and regular training

Creating awareness and regular training before and after the implementation is very important and it helps the organization to reduce the risk from confidentiality, integrity, and

availability of critical assets. Each IT or non-IT staff member in the organization can play his/her own role in ISSM. And also, we can get additional feedback from another perspective.

Testing

The ISSM is new for the majority of public organizations. Therefore, testing is very important. The organization can precede the test phase by phase. After testing the first phase there are feedbacks from the end-users. It can help to add or remove some components from it, and it can show how to implement the next phase.

Inspection

After implementation, there must be an inspection of the ISSM. It helps to identify the problems. The organizations can get the opportunity to review the implementation process and to check whether the implementation meets the objectives of the organization.

5.4. Limitation of the study

This study has some limitations. One of the biggest limitations is that the study was conducted using samples from different public organizations. The information security divisions in each organization doesn't occupied by security professionals. This would limit information about the awareness of other employees on information security.

The second limitation of the study is data collections. The study uses a qualitative method and it needs the interview thoroughly. The respondents even the security officials are not well trained in the field of security and it limits the collected information. And the study doesn’t collect end users data.

The third limitation is COVID 19. The data was collected from the mid of March up to the end of April. The time was very difficult for the respondents to meet me face to face, and the majority of them are stay at home and it was very difficult for me to get their response.

5.5. Further research

There are components of ISSM that are outside the scope of this research are recommended for further research. These are:

- How to measure the information system security management effectiveness in the context of public organization in Ethiopia. Information system security strategy, and develop metrics to be used against security goals, and objectives.
- Determining the impact level of trust, ethical conduct, and culture on the process of ISSM development and implementation in public organizations.

- How the Ethiopian public organizations develop the Information system security management culture?

References

Amarachi A.A., O. S. (25 June 2013). Information Security Management System: Emerging Issues and Prospect. IOSR Journal of Computer Engineering (IOSR-JCE), 2.

Areejalhogail, D. A. (October 2014). Information Security Culture: A Definition and A Literature Review. Conference Paper · October 2014,2-8.

Aychiluhim D., T. B. (2015). Internet Banking Security Framework: The case of Ethiopian Banking. Hilcoe Journal of Computer Science and Technology, Vol. 2, No. 2,1-7.

Bowen, G. A. (2009). Document Analysis as a Qualitative. Qualitative Research Journal, vol.9, no. 2, 2009,1-14.

(BSI), B. F. (2008).BSI - standards 100-1 Information security management system (ISMS). Bonn: BundesamtfürSicherheitin der Informationstechnik(BSI).

COBIT@2019. (2019). COBIT@2019 Introduction and Methodology .ISACA.

Commerce, N.I.(2011, March).National Information Security Risk Organization, Mission, and Information System View. NIST Special Publication 800-39. US: NIST Special Publication800-39.

Eijiroh Ohki., Y. H. (2007). Information Security Governance Framework. Research Gate, 6.

Ejerssa, n. (2018). Assessment of information security maturity level on Ethiopian public universities. Addis Ababa university,6-7.

ESSTI, April ,(https://etssti.org/home-2/)

Gebrehiwot, y. (2018).Assessing information security management using an iso27001:2013 framework:acasestudyatethiotelecom.AThesisSubmittedtoSchoolofGraduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science,14-21.

Goedvolk, H. S. (2000). The design, Development & deployment of ICT systems in 21stcentury integrated Architecture framework (IAF) Cap Gemini Ernst and Young.

Government, D. (2018).Danish Cyber and information Security Strategy 2018-2021. The Danish Government.

Heru s., m. N. (2018).Information security management systems. Apple academic pressinc.

Haufe Knut, K. B.-P. (2016). A process framework for information security management. International Journal of Information Systems and Project Management, Vol. 4, No.4, 2016, 27-47,21.

Heru, S., Mohammad, N. A., & Yong, C.T. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical& Computer Sciences IJECS-IJENS Vol: 11 No:05.

ISACA(1996).ControlObjectivesforInformationandrelatedTechnology(COBIT).Retrieved from:http://www.the281group.com/index.php/control-objectives-for-information-andrelated-technology-cobit. Accessed Date: 10 Nov2019

Institute., I. G. (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition. United States of America: IT Governance Institute.

Isaca. (2019). Cobit® 2019 framework: governance and management objectives. Usa:isaca®.

ISO/IEC 27001.(2005). Information technology, Security techniques, Information security management systems, Requirements.

ISO/IEC 27001.(2013). Information technology, Security techniques, Information security management systems, Requirements.

ISO/IEC 27002.(2013). Information technology – Security techniques – Code of practice for information security controls. In:ISO/IEC.

ISO/IEC 27005.(2013). Information technology – Security techniques – Information security risk management. In: ISO/IEC

ITU. (2018). Global Cyber Security Index (GCI). ITU Publications.

Janne J. Korhonen, K. H. (2015). Information Security Governance. Research Gate ,17.

Joobin C., G. D. (2007). Management of Information Security: Challenges and Research Directions. Communications of the Association for Information Systems (Volume20, 2007) 958-971.

Kabir, S. M. (2016). Methods of data collection. Research gate,1-77.

Kothari, C. (2004). Research Methodology Methods and techniques Second Edition. In C.R.Kothari, Research Methodology Methods and techniques (pp.2-7).New Delhi: New Age International(P) Limited Publishers.

Kelemie, T. (2013), Information Security management framework for banking industry in Ethiopia, Addis Ababa University: Unpublished Master's Thesis.

Kuligowski, C. (2009). COMPARISON OF IT SECURITYSTANDARDS).

Kristian, B., Isabelle, C., Stefan, F.,Denis, H., and Maritta, H., (2018) A Structured Comparison of Security Standards

Lee,M.C.(2015,AugustAugust10,2019).InformationSecurityManagementasaBridgein Cloud Systems. Retrieved fromwww.mdpi.com/journal/sustainability:www.mdpi.com/journal/sustainability

Maiti., S. A. (2014). Information Security – Evolution, Impact and Design Factors. International Journal of Computer Applications,6.

Myers, M. D. (2009). Qualitative Research in Business & Management'. Sage,

London.Mekonenn,D.2016

Michael, N., Kelley, D., &Victoria, Y., (2017) NIST Special Publication 800-12 Revision 1An Introduction to Information Security

MOFED. (2019, December 09).http://www.mofed.gov.et/web/guest/overview-of-the-ministry

MOR. (2019, December 09).Http://www.mor.gov.et/index.php/about-us#objective-of-authority.

Muhamet .Gerella., N. P. (2018). IT Infrastructure Library (ITIL) framework approach to IT Governance. Science direct.

Myers, M. D. (2009). Qualitative Research in Business & Management'. Sage, London.

Nakrem, A. (2007). Managing information security in organizations: a case study(Master's thesis, Høgskolen iAgder)

NIST,(July,2002) Risk Management Guide for Information Technology Systems

Omar S, F. T.-A. (2016). Information system Security Threats and vulnerabilities: Evaluating the Human factors in Data protection. International Journal of Computer Applications ·June 2016,2-3.

Salahuddin, A.(2011), Information security management A case study of an Information security culture. Queensland University of Technology.

Stuart M.,&. N. (2016).Research Methods Handbook. Centre for Local Economic Strategies.

Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling. International Journal of Academic Research in Management (IJARM),1-11.

Thomas R. Peltier., J. P. (2005). Information Security Fundamentals. Washington, D.C: AUERBACHPUBLICATIONS.

TemtimAssefa (2011) ICT Assimilation in Public service organizations of Addis Ababa City Administration: The Fourth National Conference on Managing Ethiopian Cities in Era of Rapid Urbanization: "Cities as Engines of Growth and Transformation in Ethiopia", May 31st, 2011, Addis Ababa, Ethiopia.

Tibebe B., E. B. (2017). An Investigation on the Current Information System Security Maturity.

Hilcoe Journal of Computer Science and Technology, December,6-7.

Tibebe B., S. N. (2009). The Impact of Organizational Culture on IS Implementation Success in Ethiopia: the Case of Selected Public and. Association for Information Systems AIS Electronic Library(aisel).

Tsedale, Y. (2018), Assessment of information security incident management practice in Ethiopian bank. Addis Ababa University: Unpublished Master's Thesis.

TECHIN, April,(2020).http://www.techin.gov.et/glance/

Www.solarwindsmsp.com. Retrieved fromhttps://www.solarwindsmsp.com/blog/information- security-framework#:https://www.solarwindsmsp.com/blog/information-security-framework# Solarwinds. (2019, May, 201919/11/2019).

Www.techopedia.com. (2019, November11). Https://www.techopedia.com/definition/10282/information-security-is.

www.originit.co.nz.https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/).

Yin, R. (1984). Case Study Research: Design and Methods. Beverly Hills, Calif: Sage.

Zainal, Z. (2007). Case study as a research method. JurnalKemanusiaan bil.9, Jun 2007,1-2.

APPENDICES

Appendix A: Interview Questions

1. Interview Questions for top Management HUMANRESOURCES SECURITY
2. What are the management role (of all levels) engaged in driving security within the business in the organization?
3. Does management behavior and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures?
4. Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the organization?
5. Is there a formal disciplinary process which allows the organization to take action against employees who have committed an information security breach?

2. SUPPLIERRELATIONSHIP

1. Is the management needs to have information security included in contracts established with suppliers and service providers, and in what manner do the manager reacts?
2. Is there an organization-wide risk management approach to supplier relationships in top management level?
3. Do supplier agreements include documented security requirements to address information security within the service & product supply chain?

3. ASSETMANAGEMENT

1. What are the management role in the accurate and updated inventory of all assets associated with information and information processing facilities?
2. How the management involves to ensure all employees and external users return the organization's assets on termination of their employment, contract or agreement?
3. Is there a process by which all information can be appropriately classified?

   What are the management role in a policy governing information classification, and how it looks like for ensuring information classification?

4. If you have a policy about removable media, and personal email usage, in what manner does the organization implement the policy?

Interview Questions for Security professionals

1. INFORMATION SECURITYPOLICIES

1. Is there an information system security policy in your organization? If there is a policy, is the policy properly communicated to employees and approved by management?
2. Is there a regular policy reviewing, customization and change?

2. ORGANIZATION OF INFORMATIONSECURITY

1. Is there a responsibility for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated to the relevant parties?
2. Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information or services?
3. Is there a procedure documenting when, and by whom, contact with relevant authorities (law enforcement etc.) will be made?
4. Who and how, all projects go through some form of information security assessment?
5. Does a mobile device, removable media and personal email use policy exist? Does the policy have management approval?

3. CRYPTOGRAPHY

1. Is there a policy on the use of cryptographic controls? Is there a policy governing the whole lifecycle of cryptographic keys, and who is the responsible person?

4. PHYSICAL AND ENVIRONMENTAL SECURITY

1. Is there a designated physical security perimeter, does it have suitable entry control systems to ensure only authorized personnel have access?
2. Are there any physical protection measures to prevent natural disasters, malicious attack or accidents been designed in?
3. Are environmental hazards identified and considered when equipment locations are selected, and is there a disaster recovery system?
4. Is there a UPS system or backup generator? Have these been tested within an appropriate timescale?

5. SUPPLIER RELATIONSHIP

1. What is the security professionals role in contracts established with suppliers and service providers?
2. Is there an organization-wide risk management approach to supplier relationships?
3. Do you check that suppliers provided documented security requirements; and supplier agreements include requirements to address information security within the service& product supply?

6. ASSETMANAGEMENT

1. What are the security professionals role in the accurate and updated inventory of all assets associated with information and information processing facilities?
2. How the security professionals involves to ensure all employees and external users return the organization's assets on termination of their employment, contractor agreement?
3. Is there a process by which all information can be appropriately classified?

   What are the security professionals role in a policy governing information classification, and how it look like for ensuring information classification?

7. OPERATIONSSECURITY

1. Is there any well documented operating procedures, and available to all users who need them?
2. What are the processes to detect malware in place? Does the organization have a process and capacity to recover from a malware infection and other attacks?
3. Is there an agreed backup policy? Does the organization's backup policy comply with relevant legal frameworks? Who is going to check backups made in accordance with the policy? Are backups tested?

8. COMMUNICATIONSSECURITY

1. Is there an organizational policy govern how information is transferred? If there is a policy, what are the procedures for how data should be transferred made available to all employees, relevant technical controls in place to prevent non-authorized forms of data transfer?

   Are all employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements?

Interview Questions for Other IT officers

1. ASSET MANAGEMENT

1. What are the network professionals role in the accurate and updated inventory of all assets associated with information and information processing facilities?
2. How the network professionals involves to ensure all employees and external users return the organization's assets on termination of their employment, contract or agreement?
3. Is there a process by which all information can be appropriately classified? What are the network professional's role in a policy governing information classification, and how it look like for ensuring information classification?

2. ACCESSCONTROL

1. Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role?
2. Is access to information and application system functions restricted in line with the access control policy?
3. Where the access control policy requires it, is access controlled by a secure log-on procedure?
4. Are password systems interactive, or complex?
5. Does the organization have a policy around how unattended equipment should be protect, and technical controls in place to secure equipment that has been inadvertently left unattended?

3. INFORMATION SECURITY INCIDENTMANAGEMENT

1. Is there a clearly documented and identified management responsibilities in the incident management processes?
2. Is there a process for timely reporting of information security events? Is there a process for reviewing and acting on reported information security events? Is there a process for reporting of identified information security weaknesses?
3. Is there an incident response process which reflects the classification and

severity of information security incidents?

4. Is there a process or framework that allows the organization to learn from information security incidents and reduce the impact / probability of future events?

4. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUTY MANAGEMENT

1. Is information security included in the organization's continuity plans? Does the organization's information security function have documented, implemented and maintained processes to maintain continuity of service during an adverse situation?

Appendix B: Document Analysis Checklist

S.N	Types of Document	Description
1	IT policy	Content Who is the author, and the responsible person for the implementation
2	Security Framework	Aim of the document and Content
3	Project descriptions	Types of the project and the Content of IS on it
4	Work description	Content about Security professional

Appendix C: Observation Checklist

S.N	Types of Observation	Description
1	Office	Working Environment
2	Physical environment	Equipment allocation in the offices
3	Datacenter	Data center location including all the necessary physical security