ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSING INFORMATION SECURITY MANAGEMENT USING AN ISO 27001:2013 FRAMEWORK: A CASE STUDY AT ETHIO TELECOM

By

Yemane Gebrehiwot

NOVEMBER, 2018

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSING INFORMATION SECURITY MANAGEMENT USING AN ISO 27001:2013 FRAMEWORK: A CASE STUDY AT ETHIO TELECOM

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

By: YEMANE GEBREHIWOT

Advisor: LEMMA LESSA (PhD)

NOVEMBER, 2018

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

ASSESSING INFORMATION SECURITY MANAGEMENT USING AN ISO 27001:2013 FRAMEWORK: A CASE STUDY AT ETHIO TELECOM

By: YEMANE GEBREHIWOT

Name and signature of Members of the Examining Board

Lemma Lessa (PhD)	_____	_____
Advisor	Signature	Date
Gashaw Kebede (PhD)	_____	_____
Examiner	Signature	Date
Workshet Lamenew (PhD)	_____	_____
Examiner	Signature	Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that the thesis 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. A list of references is appended.

Signature: _____

YEMANE GEBREHIWOT

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

Advisor's Signature: _____

LEMMA LESSA (PhD)

Acknowledgements

First and foremost, I would like to thank the almighty GOD for giving me the strength, courage, patience and perseverance to endure this research study.

I am so grateful for the wise council of my advisor, Dr. Lemma Lessa. I have been fortunate, to work under the supervision of such an academic man! Many thanks Dr. Lemma for your invaluable guidance, inspirational support and encouragement, as well as your patience in respect of my shortcomings.

My special thanks to my father Gebrehiwot Bezabih and my mother Tsehainesh Weldesillassie, my brothers Alem, Meareg, Haftom and Kibrom. Without your support this would not have been possible.

My special thanks to my close friends Hagos Girmay, Tesfahunegn Guesh and Senait Ayalew for giving me the encouragement with full support to keep moving forward throughout my study. Without your support this would not have been possible.

My special thanks to all research participants of Ethio telecom especially information system division who have given me time from their busy schedule. Special thanks to Tsegay Tikue, Mesfin Worku, Destaw Matebie, Yeshinegus Getaneh, Samuel Taye, Mehari Gebreegziabher, and Gebremeskel Aregay for their kind cooperation and assistance me during my study.

Finally, I must express my very profound gratitude to my beloved wife Ruta Gebreegziabher, my son Ruwyet Yemane, my daughter Luwam Yemane. Without your love, patience and support this would not have been possible. Thank you for understanding that the hours spent immersed in this effort were for good purpose, and for giving the encouragement to keep moving forward.

Yemane Gebrehiwot

November, 2018

Addis Ababa, Ethiopia

Abstract

Nowadays, information is becoming critical for any organization because information is one of the most valuable assets in organizations to operate their businesses and market interactions. Information security and its management have great role on keeping the organization's reputation through the preservation of confidentiality, integrity and availability of the systems and services in telecom sector. An information security management system is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

Despite its importance for business innovation, information technology has continuously posed new security challenges to business information and information assets. The technical solutions alone cannot be enough to address the information security challenges. Management aspects and fulfillment of information security standards are required to be considered. The purpose of this study is to assess current information security management practices of Ethio telecom based on the ISO/IEC 27001 and its control to identify the critical and mandatory requirements for ISM based on ISO/IEC270001:2013 standard for Ethio telecom. In this work, attempts were done to examine and compare the available ISM frameworks and standards. This research combines ISO/IEC 27001 audit checklist and researcher's own experience to assess the information security practices in telecom industry.

Both qualitative and quantitative research approach were used. Data were collected via questionnaire survey, document analysis, and interviews. To analyze the data SPSS tool is used. The study results show that assessed telecom is at diverse states in managing the security of its information security. Moreover, they all are found to be at low level or doesn't comply of ISM practice with respect to the selected international standard. Critical and mandatory requirements for ISM is developed and evaluated. The evaluation identifies and shows the security requirements and selects controls. Thirteen main ISM requirements are identified as critical and mandatory and also some which are not mandatory for the telecom sector.

Keywords: Information Security, Information Security Management, Information Security Management Framework

Table of Contents

List of Tables

List of Figures

List of Acronyms

COBIT	Control Objectives for Information and Related Technology
C.I.A	Confidentiality, Integrity and Availability
CESG	Communications-Electronics Security Group or National Technical Authority for Information Assurance(UK)
DMZ	Demilitarized Zone
ENISA	European Network and Information Security Agency
GTP II	Growth and Transformation Plan II
IT	Information Technology
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISMS	Information Security Management System
SPSS	Statistical Package for the Social Sciences
PDCA	Plan Do Check Act

CHAPTER ONE

INTRODUCTION

This chapter is to introduce background of the research, statement of the problem, research questions and the objectives of the research. Furthermore, the chapter describes the significance and the scope of the research.

1.1 Background

Nowadays, information is the most valuable and fundamental asset in any organization. Therefore, protecting the security of information is very important and has become a top priority for many organizations (Heru et al 2011; Teece, 2010). To protect this valuable asset, there should be a proper information security practice and management that keep information from a wide range of internal and external threats and preserve its value to the organization.

Information security is a broad subject that covers technology, operations and people to ensure integrity, confidentiality and availability of data. It also involves in our day-to-day operation of an organization to ensure the success, progress of the business and to get the customers trust besides to the competitive advantage of the business (Daniel, 2017). Securing information is required to build bridge of trust between the client of the service and the presenter of the service. Information security is related to the protection of information technology assets against the risks of loss, misuse, disclosure or damage (Rezakhani et al., 2011). Therefore, it is essential to give much consideration for information security as much as the value of the business which is determined in the value of its information. Von Solms & Von Solms (2000) notes that securing information is one of the most important aspects in any organization today and that the primary aim of information security is to protect the organization and its assets (such as sensitive information) against attempts of intrusion and corruption.

Information security management consists of a series of processes by which formal, informal and technical controls are applied to address security risks (Sveen, et al., 2009). Technical controls that include firewalls, intrusion detection systems, and other devices that regulate access to

resources. Informal controls such as training and education influence security culture (Zhi et al., 2013).

To manage information security at an acceptable level, both technical and formal controls should be put into effect. If all these controls are not in effect, risks will not be adequately addressed. On top of the controls, information security management also plays the biggest role in protecting the valuable information since, without management it will be difficult to understand what has been done, why, by whom and for what purpose (Debi, 2008). As Chang and Lin (2007), solid security products or technology alone cannot protect an organization without a good management policy and implementation. Thus, the key factors in successful information security management are the effective compliance of security policies, proper integration of people, process and technology (Emin_agao_glu, et al., 2009). In general, implementing and configuring the security tools by itself is not a solution to protect organization information unless it is properly managed. Policies and procedures should also incorporate information security in regard to people, process and technology. Security weaknesses cause a negative impact such as financial loss, reputations, and loss of customer confidence on organizations (Kumar, Park, and Subramaniam, 2008). Information security management in telecommunication is crucial.

Ethio telecom is the only company that is providing telecommunications service in Ethiopia. It is one of the major financial contributors to the Ethiopian government. This company is providing telecom services, voice, data and video for more than 57 million customer base (Africa news, 2017) and has big investment by Growth and Transformation Plan II (GTP-II) in different telecom technologies such as third generation (3G), fourth generation (4G) and broadband technologies. Moreover, the company has big infrastructure in datacenter, virtual internet service provider and hosting services for a large number of customers. Based on the preliminary assessment the researcher has conducted, there is no standardized and formal information security management practice at Ethio telecom. Due to this reason, the company is losing big money such as internal and external telecom frauds. Therefore, for this company formal information security management is not an option but it is mandatory for its existence. Thus, this research focuses on assessing the current practice and to identify the critical and mandatory requirements for ISM based on standards for Ethio telecom.

1.2 Statement of the Research Problem

Currently organizations depend on information for their survival (Whitman and Mattord, 2004). Specifically, organizations depend on the systems and controls in place that provide for the ongoing confidentiality, integrity, and availability of their data and information (Krutz and Vines, 2004). According to Caralli (2004) many organizations are ill-equipped to define their security goals let alone to make an explicit connection between their security goals and the strategic drivers of the organization. Schneier (2004) states that threats to organizational information and information systems are increasing in occurrence and complexity and emphasizes the urgency for organizations to learn how to better protect their information assets.

Telecommunications have emerged as one of the strongest driving forces and a rapidly growing industry across the world with a unique set of business requirements and challenges much larger in scale and complexity as compared to traditional businesses (QAI Global Services, 2014). The current era of rapid technological advancements has posed new threats to business information and information assets at every stage of information life cycle (i.e. information generation, processing, storage and distribution) for organizations. Many high-end technological solutions have been proposed and implemented to deal with this situation. However, information security still remains a serious challenge.

Businesses find themselves in need to adopt standards for various reasons which vary from business requirements to regulators and compliance mandates. Establishment of proper corporate governance, increasing risk awareness and competing with other enterprises are some business drivers to mention. Some firms follow certifications to meet market expectations and improve their marketing image (Al-Ahmad & Mohammad, 2013). Security compliance is one of the major issues in information security management(ISM). Due to this, many different framework, guidelines, and standards were proposed by researchers, practitioners, consultants, and professional organizations to protect their information assets (Choobineh et al., 2007). The use of security standards in companies or government agencies not only improves the level of security, their use also makes it easier for organizations to agree on which security safeguards must be implemented in what form. The number one priority for making compliance work is assessment and evaluation. If the

company weaknesses are not known in terms of information security then this makes it nearly impossible to put the best practices into action (Susanto & Almunawar, 2015).

However, the limitation of the standards arises precisely from their generality and thus they fail to pay adequate attention that organizations differ and therefore their security requirements might differ .There is an opposition between the generality of standards, and the organization-specific nature of ISM . In addition, as standards are generic, business requirements proposed by the standards may involve conflicts with the organization's normal business requirements (Barlette & Fomin, 2010). The effective management of security risks ultimately requires appropriate implementation of information security management .Security management is more effective when it is applied in context of business requirements and balanced against the organizations adopted risk posture (Lane, 2007).

Several standards exist to aid in information security. Out of all these standards, ISO 27001 is the most used (Heru et al., 2011 & ENISA, 2012). ISO 27001 can be viewed as an overall program that combines risk management, security management, governance and compliance. It helps the firm ensure that the right people, processes and technologies are in place, and facilitates proactive approach to managing security and risk (Brenner, 2007).The ISO/IEC 27000-family focus on what to do when it comes to ISM. The step from knowing what to do and to understand how to do it has proved to be overly complex and costly for many organizations (Gillies, 2011). The ISO/IEC 27000-family is intended to assist organizations of all types and sizes with implementation and operation. So that telecom industry followed the competition in the market increased the information security risk and fraud, it is compulsory for the organization to follow international standardized ISM which is suitable to their organizational context in order to be world class operator as it is stated in the vision of the organization.

According to a preliminary survey conducted on assessing ISM practices in Ethio telecom, ISM adoption is gaining momentum but is still in the early stages of implementation for the company. Adoption of the ISM framework (guidelines, principles, and concepts) is either absent or is still being established and is not yet fully implemented. So, that is why this study focused on identifying the critical and mandatory requirements for ISM based on ISO 27001:2013 standards for Ethio telecom. Besides most of the researches done about ISMS has been performed in technologically developed countries. On top of this, information security major international standards are written

from a western perspective, without knowing how applicable ISM concepts and practices to other cultures, which has different social, organizational, and security cultures (Mohammed et al., 2009).Organizations need to establish new security business structures based on their integrated architectural approach to operate in a distributed, heterogeneous and multi-disciplinary business environment. It is necessary for such an Architectural approach to include the issues Policy, Risk, Objectives, Technology, Execution, Compliance and Team (Nakrem, 2007). Thus, the purpose of this research is to assess the current ISM practices of Ethio telecom and identify the critical and mandatory requirements for ISM based on ISO/IEC270001:2013 standard for Ethio telecom

1.3 Research Questions

In this study, the researcher aims to answer the following research questions which are designed to achieve the research objectives.

- What is the current status of information security management(ISM) practice in Ethio telecom?
- What are the Security gaps from the perspective of ISO/IEC 27001:2013?
- How can we identify the critical and mandatory requirements for ISM based on ISO/IEC270001:2013 standard for Ethio telecom?

1.4 Objectives of the Research

1.4.1 General Objective

The general objective of this research to assess the current ISM practices of Ethio telecom and identify the critical and mandatory requirements of ISM based on ISO/IEC 27001:2013 standard.

1.4.2 Specific Objectives

- To identify the existing information security management practice in Ethio telecom.
- To identify security gaps from the perspective of ISO27001:2013.
- To identify the critical and mandatory requirements of ISM based on ISO/IEC 27001:2013 standard which can enable the direction to manage information security at Ethio telecom.

- To suggest recommendations for management on how to go with implementation of the identified critical and mandatory requirements of ISM.

1.5 Significance of the Study

The findings and results of this research may be of potential value to the Ethio telecom, it provides new insights of information security management. Based on the identified critical controls influencing the implementation of information security management system at providing the necessary considerations to be undertaken by Ethio telecom in identify their security risk areas and take measures based on the recommendation of this study. In addition, it may identify the critical and mandatory requirements for information security management and serve as a bench mark for better security and delivering secured service. The study will be used as the springboard for other researchers for future work on the domain area.

1.6 Scope of the study

Currently, information security has become very critical, different studies have been accomplished in different time to address issues related to the subject by different scholars. The studies which had been previously conducted mostly focused on the general information security management of organizations such as banks using international security standards as a measurement instrument and recommend best practices accordingly.

This study however, assesses the current practice of information security management in Ethio telecom specifically in information system division (ISD) using ISO/IEC 27001:2013 security standard framework as a major instrument to measure the current stand of the organization. In related to information security management practice, literature review in information security and provide a roadmap towards security compliance. Regarding the limitation of this study, being a single case by itself is limitation and information related to information security is much more confidential and sensitive in the telecom industry. Thus, as information at the telecom sector is very confidential and sensitive, it needed effort and continuous communication with the telecom security management to convince as their information wouldn't be disclosed to any third parties for the sake of their reputation. Involving other divisions of Ethio telecom their input that could be very relevant was not covered due to the need of ample time and budget for a better analysis result.

1.7 Operational Definitions

The following list of terms provides definitions derived from the selected literature as a way to reveal specific context concerning the topic of information security management.

Access Control - The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities.

Business continuity - The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event or interruption.

A data center: is a facility that centralizes an organization's IT operations and equipment, as well as where it stores, manages, and disseminates its data. Data centers house a network's most critical systems and are vital to the continuity of daily operations.

Security patch management: security patch management process has become a critical component in the maintenance of security on any information system. As more and more software vulnerabilities are discovered and therefore need updates and patches, it is essential that system administrators manage the patching process in a systematic and controlled way. Information security responsibilities

De-Militarized Zone (DMZ): is a special local network configuration designed to improve security by segregating computers on each side of a firewall. It is a physical or logical sub-network that separates an internal local area network from other untrusted networks, usually the Internet.

Control - Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature NOTE: Control is also used as a synonym for safeguard or countermeasure.

Critical Elements - Elements which ensure business continuity, minimizing business risk, and maximizing return on investments and business opportunities.

Cryptography - The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity.

1.8 Organization of the Study

This research is organized in five chapters. These include:

Chapter 1: It introduces the background of the company, the value of information assets, security and management in relation to the telecom sector specifically in information security management with respect to the ISO 27001:2013 standard. The chapter also includes statement of the problem, research questions, and research objectives, significance of the study and scope of the study.

Chapter 2: In this chapter, literature in information security, information system vulnerability, information security threats, common information security attacks, information security risk assessment and management, information security management, information security management roles, information security management process, information security management certification, information security risk in the telecom sector, information security management in the telecom sector, information security management standards and best practice, information security governance, information security compliance and finally, ISO/IEC 27001:2013 is reviewed and discussed thoroughly to provide an overview and explore the topic.

Chapter 3: this chapter describes the research design and methodology used. Thus, the chapter includes, research design, source of data, sampling technique, research population , data collection methods, sample design , validity, reliability, Statistical data analysis and ethical consideration.

Chapter 4: in this chapter, the collected data is analyzed, interpreted, described and discussed based on the significance of the key findings in light of what was already known about the research problem.

Chapter 5: this chapter concludes the research and provides recommendations and Limitations as per the findings.

CHAPTER TWO

LITRATURE REVIEW

INTRODUCTION

This chapter examines with the review of related literature on nature of the current approach to information asset, information security and its management (or information security management system), information security standards/frameworks in the organizations especially in telecom sector and then dives to the international standard (ISO 27001:2013) in detail. Finally summary of this chapter.

2.1 Information Asset

Nowadays, information is the most valuable and fundamental asset in any organization. Therefore, protecting the security of information is very important and has become a top priority for many organizations (Heru et al., 2011; Teece, 2010). To protect this valuable asset, there should be a proper information security practice and management that keep information from a wide range of internal and external threats and reserve its value to the organization.

According Karamanlis (2016) Organizations of all types and sizes (including public and private sector, commercial and nonprofit) store, collect, process, and transmit information in many forms including physical, electronic and verbal. The value of information goes beyond the written words, numbers and images. Knowledge, concepts, ideas and brands are also examples of intangible forms of information. In the globally connected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various threats. He also highlighted that Information is a crucial resource for all organizations, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become unescapable in enterprises and in social, public and business environments. As a result, organizations and their executives attempt to maintain high-quality information to support business decisions and embrace the management of information like any

other significant part of doing business. To protect this essential asset, there should be a proper information security practice and management that keep information from a wide range of internal and external threats and reserve its value to the organization.

2.2 Information Security

With the fast development of information technology, personal computers, telecommunication, and the internet, makes people to access information anywhere and anytime. Though most of people obtain this information legally, some hackers have been trying to bypass the security gaps and attack the computer systems .The attack could come from either the external or the internal organizations. The attack can either be Denial of Service (DoS) or be big damage of the whole framework. Due to this, the concept of information security has become a big issue for the whole world (Farn, et al., 2004).

Information security is a broad subject that covers technology, operations and people to ensure integrity, confidentiality and availability of data. It also involves in our day-to-day operation of an organization to ensure the success, progress of the business and to get the customers trust besides to the competitive advantage of the business (Daniel, 2017).Every organization is faced with the task of providing a comprehensive plan for information security. Caralli & Wilson (2004), opined that "modern organizations have a huge challenge on their hands as they must secure the organization in the face of increasing complexity, uncertainty, and interconnection brought about by an unprecedented reliance on technology regarding legislative policies on security".

The scale and scope of information security has changed over time. Initially, information security referred to a technique, but its meaning has expanded over the years. It now has a business orientation in organizational contexts (Anderson, 2003) and a comprehensive social–technique philosophy view (Zafar and Clark, 2009). Information security is given various definitions by different scholars. The following is a list of some seminal definitions of information security from the technique perspective:

I. 'Computer security rests on confidentiality, integrity and availability', which are the three components of computer security (Bishop, 2003).

II. 'Information security is protecting confidentiality, integrity and availability of information' (ISO/IEC, 2005b).

III. ‘Information security encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets’ (Peltier, 2010).

The three definitions above emphasis on the control of information security technology. The three essential information security requirements of Bishop (2003) and the ISO/IEC (2005b), and the access control on unauthorized or accidental events of Peltier (2010) highlight an organization used to focus on technique issues rather than management issues of information security. Anderson (2003) argued that the old-style technical definition of information security creates ‘a large gap between theory and reality’, and this gap causes managers to struggle with how to manage information security in the organizational context. Therefore, he developed the following definition of enterprise information security from a management-oriented view: ‘A well informed sense of assurance that information risks and controls are in balance’.

Zafar and Clark (2009) stated that, the current definition of information security demonstrates that information security is not only a technology issue, but also an organizational and social one that accompanies the business development objectives of organizations. The social and organizational factors are important for ensuring information security in information systems because information systems are designed, implemented, maintained and used by human beings in a dynamic organizational environment (Hu et al., 2007). Nowadays, the security approaches aim to ‘deliver real business benefits’ through facilities that control information and manage risks in a dynamic environment within organizations (Ashenden, 2008).

As Michael Whitman and Herbert Matthord (2011) stated in their publication “Principles of Information Security”; successful organizations should have different layers of security in place to protect its operations:

- ***Physical security:*** There should be physical security measures in place for protecting physical items, objects zones from not entitled – unauthorized access.
- ***Personnel security*****:** Also there must be security measures for personnel security which aims to protect the individuals who are entitled to access the organization as well as its operations.

- ***Operational security*:** For protecting the details of series of activities from unauthorized individual or groups, there must be operational security measures.
- ***Network security***: communications security: For protecting all kinds of media, content and communication technology, there should be measures for communications security.
- ***Physical and logical security*:** For protecting physical and logical connections, contents and other networking components, there should be network security measures.
- ***Information security measures*:** For protecting the information assets in different perspectives such as C-I-A; even information asset is in storage (physical) stage as well as it is in operational (processing) or transmission (network) state; there should be information security measures. (Whitman & Matthord, 2011)

Protecting information from different threats to maximize business continuity and return on investments as well as minimizing risks related to business operations is called information security. It includes computer, data and also network security as there are different areas of information security management as shown in figure 2-1 *(*Aydoğmuş, 2010).

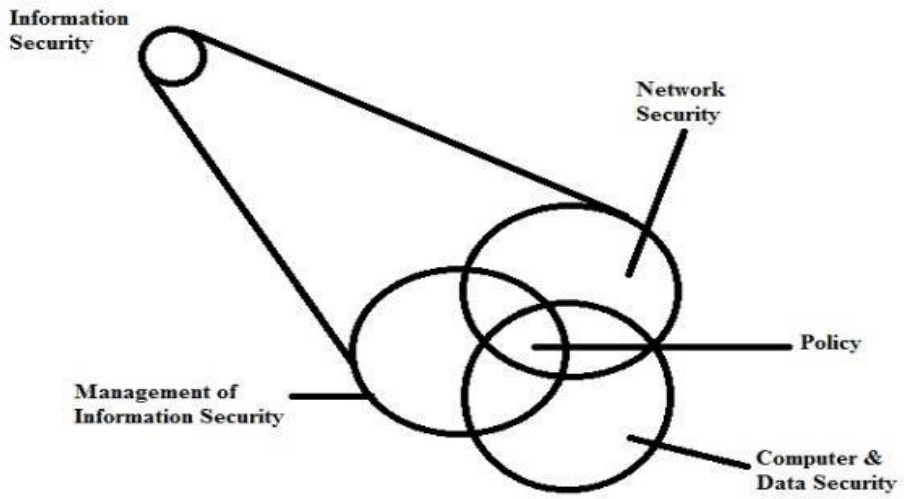

Figure 2-1: Components of Information Security (Aydoğmuş, 2010)

Therefore, in the present research, information security is defined as a system of technologies, procedures, processes and policies for ensuring the confidentiality, integrity and availability of organizational information assets in the dynamic social and organizational context.

2.2.1 Information Security Strategy (ISS)

Strategy is a concept that has evolved from a military setting where it is best described as: deciding what means to use, how to use it and how to apply it .From a business perspective define strategy as "deciding on where you want your business to go and figuring out how to get there" (Ahmad et al., 2014). These definitions can be directly applied to information security strategy. Based on these perspectives (Park and Ruighaver, 2008) define information security strategy as the "art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defense organization's information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective".

In addition, Information security strategy is defined by Beebe and Rao (2010) as "the pattern or plan that integrates the organization's major IS security goals, policies, and action sequences into a cohesive whole". These authors believe information security strategy in organization is a documented plan which matches an assessment of external cyber threats with a financially-informed set of internal countermeasures, including the required supporting policies and procedures. Strategy is seen as the means to influence an organization's environment through the careful selection of internal controls.

2.2.2 Information Security Governance (ISG)

Governance of information security is the main supporting tool for aligning objectives and strategies for information security with business objectives and strategies, and requires compliance with legislation, regulations and contracts (ISO, 2012). Alves et al. (2006) defined information security governance as act of directing and controlling an organization aligned with the strategy and business objectives, establishing and retaining a culture of information security, optimizing the related processes, and assigning activities to the most competent people to perform the

necessary actions. Implementation of Information Security Governance programme has the potential to make IS function visible for business stakeholders and ensure long-term alignment with organization's strategic goals.

Information Security Governance (ISG) should be the responsibility of top management or members of the board, as they should have authority to direct, monitor and communicate strategic goals. The governing body is ultimately accountable for ensuring an effective information security strategy and support it through appropriate information security assurance framework. In respect to information security, the key focus of the governing body should be to ensure that the organization's approach to information security is efficient, effective, acceptable and in line with business objectives and strategies giving due regard to stakeholder expectations (ISO, 2012).

According Johnston, A. C., & Hale, R. (2009), provides empirical evidence in support of an ISG program as an important condition for the success of an information security program. It also adds support for the concept that information security provides benefits to firms when addressed as an enterprise issue and integrated into executive planning and strategy. While an ISG program may be approached by some organizations as part of a regulatory compliance strategy, the advantages to firms are wider in terms of supporting organizational objectives and effectively managing risk.

2.2.3 Information Security Compliance (ISC)

Information security compliance refers to the effective implementation of information security policies and standards for protecting information in organizations. The rapid development of ICT and the increasing adoption of information systems in organizations lead to a wide adoption of information security compliance for adequately protecting organizational information (Al-Kalbani, 2017). A British Standard Institution survey (BSI, 2016) shows that more than 63% of the organizations regard information security compliance as a prerequisite for business growth while about 56% of the respondents believe that the use of an information security compliance approach in their organizations has enhanced their business operational processes.

Security compliance is one of the major issues in information security management(ISM). Due to this, many different framework, guidelines, and standards were proposed by researchers, practitioners, consultants, and professional organizations to protect their information assets

(Choobineh et al., 2007). Organizations should be compliant with one of the internationally recognized security standard to make their business expand at an international level on top of protecting their information from being exposed to external parties and which will cause security risk. The use of security standards in companies or government agencies not only improves the level of security, their use also makes it easier for organizations to agree on which security safeguards must be implemented in what form. The number one priority for making compliance work is assessment and evaluation. If the company weaknesses are not known in terms of information security then this makes it nearly impossible to put the best practices into action (Susanto & Almunawar, 2015).

According Dinesh (2015), ISO 27001 compliance (ISMS Implementation) is the general thought which everyone get is that it is the responsibility of the CISO or CXO of the organization to put things in place. They feel that security team of an organization needs to own up the implementation and are responsible & accountable for getting the organization certified. Though Information security team plays the front ending role of putting perspective in place, one needs to understand that ISMS Implementation is more of a top management driven initiative and it's a top down approach. Unless the management intends to put security in place through policy, procedures, standards and guidelines it cannot be advocated across and driven by the information security team to achieve this compliance.

It a big task to convince the organization's top management to have the ISO 27001 ISMS Implementation taken up by citing its benefits and results, on the other hand to convince the management for necessary funding to take it up. They would question about its cost, time period of implementation, its Return on Investment (ROI) etc. They are right in their own sense, because organization and top management talk and understand the language of profits and losses and not about security and compliance. The decision of ISMS Implementation will come down to balance between the investment and corresponding business benefit (Dinesh, 2015).

2.3 Information Security Management

The current literature has no universal definition for Information security management(ISM), as Information security management has developed over time and can be explained from different

perspectives, including managerial, strategic, social, socio-technical and socio-organizational (Chooineh et al., 2007). In the mid-1990s, when computers and information systems were largely used in business activities, some researchers started to be concerned with the managerial perspective of Information security management (Hou, 2014). On the other hand, Cazemier et al. (2000) defined ISM as a management process that manages people, policies, projects, programs, IT/IS facilities and resources to achieve organizational business objectives. Other researchers suggested that ISM can also be a strategic approach that helps organizations to identify optimal measurements when information security resources and budgets are limited (Finne, 2000; Gordon and Loeb, 2002).

Solid security products or technology alone cannot protect an organization without a good management policy and implementation. It is stated that information security is not primarily a technical problem but a management or business issue. The overall purpose of ISM is to enhance the confidence and the effectiveness of information services within an organization, or between an organization and its external business partners (Ernest Chang & Ho, 2006).

Understanding information security management starts with understanding characteristics of information that makes it valuable. Value of an information is based on the C.I.A. triangle. However, up to date organizational needs made these three attributes alone insufficient because of scope limitations and cannot cover the environment of the IT industry changed from day to day. With the change in industry, there are extended attributes and processes that includes identification, privacy, authentication, authorization and accountability. (Whitman & Matthord, 2011).

Confidentiality: Information shall be transferred to people on a need to know basis i.e. to keep the information from reaching to unauthorized people.

Integrity: Information stored in the computers should be kept guarded from being corrupted or contaminated.

Availability: Ensuring the availability of the data to the authorized people at right time. Both confidentiality and availability ensures data integrity.

***Identification*:** Identity is a data set that has information on subject's relationship to other entities and which has description of a person or an object uniquely. It is the first step in gaining access to

secured material. Identification is typically performed by means of a user name or other ID that is unique to each and every individual, and serves as the foundation that is essential to establish the level of access or authorization.

***Authentication*:** Authentication is the process of identity verification for a user, computer, device, service or other identity. In digital life examples of authentication includes the hardware solutions like hardware tokens or biometric scanners but also software solutions like cryptographic certificates to establish Secure Sockets Layer (SSL) connections to confirm a user's identity.

***Authorization*:** Authorization occurs after the authentication completes. It is the process that determines whether to grant or deny a user requested level of access to a resource (like access, update, or delete the contents). Access control lists and authorization groups in a networking environment and database authorization scheme to verify that the user of an application is authorized for specific functions such as read, write, create, and delete are examples of authorization.

***Accountability*:** Accountability can be mentioned as the answerability of a named person or automated process. A common example of a system that provides accountability is audit logs that track the activity of a user.

2.3.1 Information Security Management Roles

The dramatic increment in the online business opportunities are the result of the information technology; however these opportunities have also created serious risks in relation to information security. Previously, information security issues were studied in a technological context, but growing security needs have extended researchers' attention to explore the management role in information security management (Soomro, et al., 2016). The management role in managing information security is imperative as they have much influence in approving the budgeting and direct the implementation of policies and procedures that manages information security related to the business objectives.

Management of information security is primarily concerned with strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation, and maintenance of an organization's information security program (Choobineh, et al., 2007). Some of the most salient issues include asset valuation, auditing, business continuity planning, disaster recovery planning,

ethics, organizational communication, policy development, project planning, risk management, security awareness education/training, and various legal issues such as liability and regulatory compliance. Ideally, information security management activities should be driven by organizational objectives so that no resources are expended on security without an explicit documented understanding of how it supports the organizational mission (Choobineh, et al., 2007).

All the controls including logical, technical and administrative, which uses to manage information security in the organization, should be properly integrated to address the security issue related to the business objective of the organization. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and may be ineffective without being supported by appropriate management and procedures within the context of an ISM. Integrating security into a functionally complete information system could be difficult and overpriced.

In consideration of the importance, many outstanding institutes such as published information security guidelines and standards for protecting the confidentiality, integrity and accessibility of information. If firms follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment. That is, firms could safeguard their business value and benefit from IT according to the well-developed information security management (Shi-Ming, et al., 2006).

And the board of directors and the top management have a direct responsibility to ensure that all information resources of the company are secure and such security has to be maintained by the due diligence from all units at all levels throughout the whole organization. In general, organization needs to have suitably designed and implemented management structures and practices to protect its information asset, which is very important to the organization and can serve as a powerful weapon to survive a highly competitive environment (Chang and Ho 2006).

2.3.2 Information Security Management Process

Humphreys (2008), emphasized the importance for an organization to check the effectiveness of the practice of information security management. Organizations realize this by establishing a measurement process to measure and assess the effectiveness of the controls in protecting their information assets. Recently, many companies are continuously investing in information security

management as a means to improve the information security management process so as to protect the enterprise's information assets and strengthen their competitiveness since, considering the social responsibility of enterprises according to class action suits against accidents of personal information leakage, the issue of information security is accepted as a matter of survival for the enterprise (Park, et al., 2010). In the current competitive business environment, it's not only hackers and cyber criminals that hunt for information but organizations that make similar business also do these activates to understand the business strategy and business plan to disrupt the business and get advantage of it.

In general it is very important that an organization is able to check how effective its information security management is in practice. In order to enable this to happen, the organization needs to establish a measurement process to be able to measure and assess how effective the controls are at protecting their information assets (Humphreys, 2008).

2.4 Information Security Management Certification

Information security is important for every company within all areas of business. Organizations today can't deny the importance of keeping their information secure. Having an information security management system (ISMS) that is certified on the basis of the international ISO/IEC 27001 standard shows that the organization manages its information properly and systematically thus keeping your information correct, easily accessible and well protected.

As it is explained by Park et al., (2010), there are four major motivations or benefits of enterprises attaining information security management certification. First, when an enterprise receives Information security management certification, there are positive public relations effects of better corporate image, followed by additional customers, resulting in sales increase. It showed that preventing intrusions would have cost saving effects as damage from potential accidents can be prevented. Second, attaining information security reliability affects an increase in transaction stability. While information security management certification directly affects an increase in corporate value, attaining the information security reliability affects transaction stability, thus helping the stability of the information assets of the enterprise. Third, attaining information security reliability positively affects an increase in trust and fourth, increasing information security awareness positively affects an increase in security awareness. Having the certification provides

motivation for all employees and thus affected strengthening employee capability and awareness of information security. According to Dejan (2015), Telecommunication companies, including Internet providers, are very keen on protecting the huge amount of data they handle and reducing the number of outages, so naturally they look toward ISO 27001 as a framework that helps them do that. Further, similar to the financial industry, there are a growing number of laws and regulations for telecoms, where ISO 27001 is very helpful for compliance.

2.5 Information Security Risk in the Telecom Sector

The Telecommunication industry contains a lot of complexity which derives from network elements being owned by different vendors, such as proprietary applications, different operating systems, and procedures that seem unfamiliar for non-Telecom organizations. In fact, this case becomes even more complicated when Telecom operators are supplied with equipment from different manufacturers and when the network management is outsourced, which means that there will be multiple network vendors. Danielito (2012) suggested that, the imports of telecom equipment from other countries that are antagonistic to a state's strategic interests may lead to supply chain impurity by means of embedded logic bombs and malware. The dependence on telecommunication networks and the critical role that they play in the economic growth of a country has led to government regulations in the telecom industry, which include requirements for ensuring the security of the telecom equipment, networks and customer information.

The interconnection of the PSTN networks of fixed and mobile phone systems and the next generation network has increased the attack surface of the telecom networks. The wide range of end-user devices that can now connect to the telecom networks has added to the complexity of the networks, thereby increasing the risks and vulnerabilities as well (Danielito, 2012). It is well-known, as the consequences of not implementing adequate security measures to deal with these could be heavy and catastrophic to business. The biggest security threats to the telecommunication industry stated in the table 2-1 below. The possibility of information security risks is present in all telecom organizations, however, the ability to ease and overcome these risks depends on the experience and maturity that operators have.

Threat	Result
Abuse of lawful interception device	Illegal interruption of network traffic by unauthorized employees
Interruptions in the operational network	Unlawful changes to the network users' profiles, billing system, causing toll fraud and loss of credibility
Customer information in network database being compromised	Unlawful access to the customers personal and confidential information
Camouflaged as legal users, having access to their credentials by using inappropriate tools, (i.e. hacking, social engineering)	Illegal access and privileges to the network systems which then can be used for other attacks
Usage of false and modified base stations to tempt users to use it	Rejection of service, interruption of traffic
Illegal traffic exploration – observing the calling and called numbers in the network	Implication of actions that can be used possibly against Telecom Industry or customers

Table 2-1: Security threats to the telecommunication industry; adapted from (Ardian, 2016)

2.6 Information security management in the Telecom Sector

During the last few years, the Telecom industry has gone through a substantial development period and is aspiring to reach even higher levels of growth by exploring new possibilities in the market. Vastly, this industry has become a quite important piece in the giant puzzle of social interaction. Telecommunications have emerged as one of the strongest driving forces and a rapidly growing industry across the world with a unique set of business requirements and challenges much larger in scale and complexity as compared to traditional businesses (QAI Global Services, 2014).

Along with this significant expansion in the Telecom industry, the need for implementing a Security Management System has had an increase as well. This significant increase is based on the fact that telecommunication companies are prioritized to protect the huge amount of data that they possess and reduce the number of outages. Thus, these companies have requirements which include being strict and legal, in terms of their information security management. Consequently,

if there is no shield to protect telecom from various networking threats; it could result in network services becoming unreliable and even losing integrity.

Telecom operators should adopt a robust, managed security program to ensure that their networks are protected against malicious attacks, both external and internal, while also ensuring compliance to the local regulatory environment. This requires a holistic approach to implementing security measures, based on globally accepted security standards and best practices. A multi-pronged approach to security should be adopted by telecom operators to address the current and future security challenges. Industry-recognized standards, best practices and technologies must be adopted to build a robust security program. In addition, all applicable legal and regulatory requirements should also be considered. Ethio telecom is the only company that is providing telecommunications service in Ethiopia. It is one of the major financial contributors to the Ethiopian government. This company is providing telecom services, voice, data and video for more than 57 million customer base (Africa news, 2017) and has big investment plan by Growth and Transformation Plan II (GTP-II) in different telecom technologies such as 3G, 4G and broadband technologies more over the company has big infrastructure in datacenter, virtual internet service provider and hosting service for a large number of customers.

2.7 Information Security Management System Frameworks and Standards

Many organizations have implemented a large number of different security controls as a part of their information security work, trying to keep the organization secure. There are currently more than 1000 standards (Department for Business, 2013) in the information security field focusing on different aspects, from technical standards to comprehensive standards covering broader areas of information security, as with, for example, information security management standards.

To protect information and other associated assets, organizations have a set of information security measures recommended by international standards and models widely accepted by professionals and organizations around the world. Sêmola (2014) points out that each organization has its own characteristics that lead to particular Information Security needs. Organizations need to conduct a risk analysis and assessment to identify vulnerabilities, threats, probability of occurrence and potential impact, allowing them to select which measures are necessary to their own reality. Businesses find themselves in need to adopt standards for various reasons which vary from business requirements

to regulators and compliance mandates. Establishment of proper corporate governance, increasing risk awareness and competing with other enterprises are some business drivers to mention. Some firms follow certifications to meet market expectations and improve their marketing image (Al-Ahmad & Mohammad, 2013).

Some private and government organizations developed standards bodies whose function is to setup benchmarks, standards and in some cases, legal regulations on information security to ensure that an adequate level of security is well-maintained, to ensure resources used in the right way, and to ensure the best security practices adopted in an organization. For this, the five big standards are the most widely used standards for information security such as ISO27001 (International Standard Organization), BS 7799 (British Standard), PCI-DSS (Payment Card Industry Data Security Standard), ITIL (Information Technology Infrastructure Library) and COBIT (Control Objectives for Information and Related Technology) (Heru et al., 2011).

These standards such as ISO 27001 and BS 7799 focusing on information security management system as main domain and their focus on, while PCI-DSS focus on information security relating to business transactions and smart card, ITIL and COBIT focuses on information security and its relation with the Project management and IT Governance. Each standard playing its own role and position in implementing ISMS (Heru et al., 2011).Organizations which have published information security standards and gained great acceptance includes International Standardization Organization (ISO), Information Systems Audit and Control Association (ISACA), Information Systems Security Association (ISSA), National Institute of Standards and Technology (NIST), British Standards Institution (BSI), Information Security Forum (ISF), Payment Card Industry Security Standards Council and others.

Some security standards are continuously published and gain acceptance; some of them provide guidelines, others promote best practices, while a few can be used as a basis for certification (Daniel, 2017). Therefore, by adopting industry best practices (e.g. CobiT, ISO 27000, PCI-DSS) and adjusting IT infrastructure with high-level executive objectives, companies can lower IT risks, especially security and operational risks (Spremic, 2011).

2.7.1 ISO/IEC 27001

ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government; also other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations whereas BS (British standard) Standards is the UK's National Standards Body (NSB) and was the world's first. BS Standards works with manufacturing and service industries, businesses, governments and consumers to facilitate the production of British, European and international standards. According IT Governance Ltd (n. d.) ISO/IEC 27001 is the international standard that describes best practice for an ISMS (information security management system). Achieving accredited certification to ISO 27001 demonstrates that the company is following information security best practice, and provides an independent, expert verification that information security is managed in line with international best practice and business objectives. ISO 27001 is supported by its code of practice for information security management, ISO/IEC 27002(ISO, 2013).

2.7.2 PCI DSS

Payment Card Industry - Data Security Standard (PCI DSS) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council (Heru et al., 2011). The standard was created to help industry organizations processes card payments and to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands (Heru et al., 2011). Generally, it is security controls for credit card transactions.

2.7.3 COBIT

Control Objectives for Information and related Technology (COBIT) is a certification created by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996 (Heru et al., 2011). They believe that it is a set of practices (framework) for IT management. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues (Heru et al., 2011). It presents an international and generally accepted IT control framework

enabling organizations to implement an IT governance structure throughout the enterprise (Yigezu, 2011). On the other hand, COBIT describes a method for controlling the risks arising from the use of IT to support business-related processes (BSI-standard 100-1, 2008). Further, form currently available standards, only COBIT addresses the full spectrum of IT governance duties (Jimmy, 2012). 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).

2.7.4 ITIL

The Information Technology Infrastructure Library (ITIL), is a best practice framework for IT service management. ITIL was developed by the Central Computing and Telecommunications Agency – today Office of Government Commerce in Norwich (England) developed on behalf of the British government. According Haufe (2016), IT service management is the management of all processes that co-operate to ensure the quality of live IT services, according to the levels of service agreed with the customers .The primary objective of service management is to ensure that IT services are aligned to the business needs and actively support them.

		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
1.	Information Security Policy	√	√	√	√	√
2.	Communications and Operations Management	√	√	√	●	√
3.	Access Control	√	√	√	√	√
4.	Information Systems Acquisition, Development and Maintenance	√	√	√	●	√
5.	Organization of Information Security	√	√	√	√	√
6.	Asset Management	√	√	√	√	√
7.	Information Security Incident Management	√	●	√	√	√
8.	Business Continuity Management	√	√	√	√	√
9.	Human Resources Security	√	√	√	●	√
10.	Physical and Environmental Security	√	√	√	●	√
11.	Compliance	√	√	√	√	√

Table 2-2: The big five standards; adapted from (Heru et al, 2011)

ISO's most widely used in globally, compared with BS, PCIDSS, ITIL and COBIT. Indication descript us that ISO is more easily implemented, stakeholders (clients, suppliers, customers and management) is easier to recognize, also it has appropriate platform in an organization deal with, than four others security standards (Heru et al., 2011).In addition to this comparative study, Survey analysis was conducted by the European Network and Information Security Agency (ENISA) to seek standards and good practices that are in use in the EU (European Union) telecommunications market. As a result, ISO/IEC 27001 is considered being the best practice.

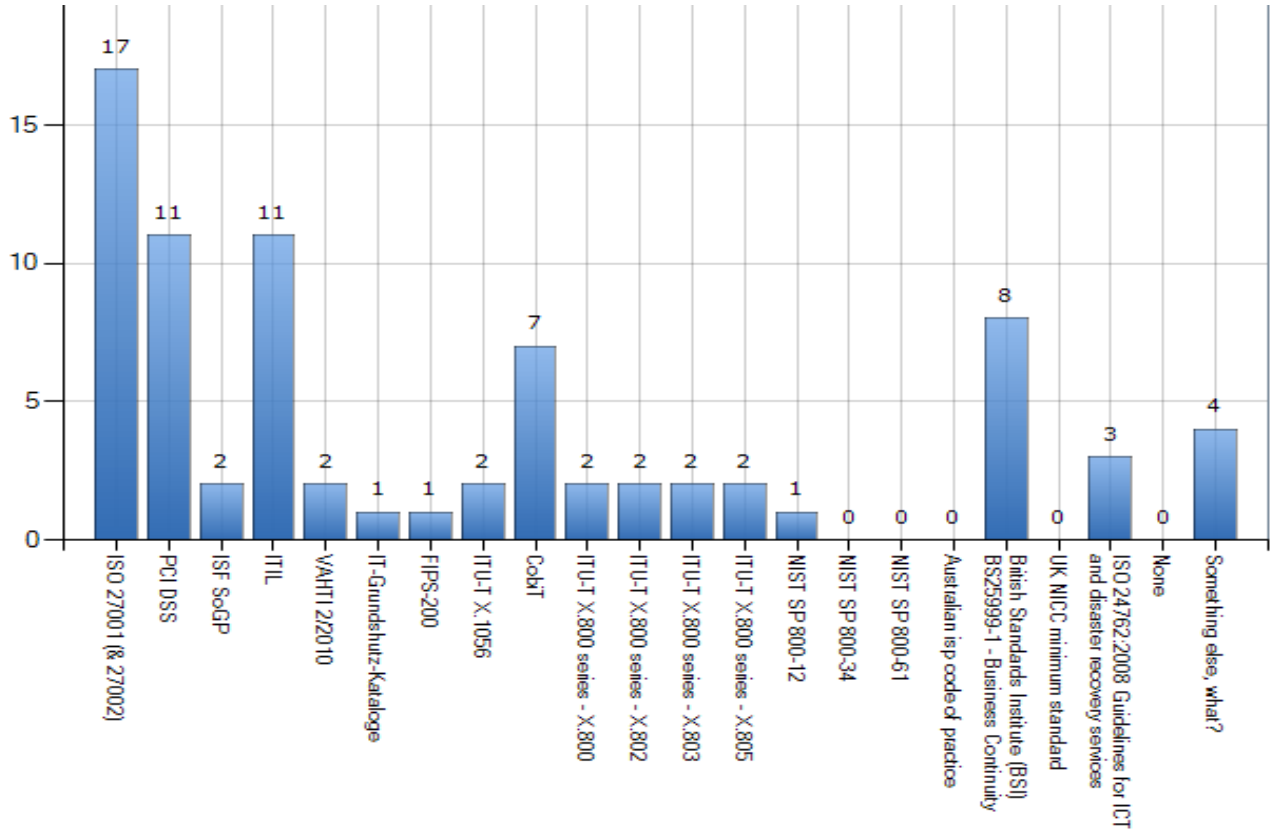

Figure 2-2: Standards used by organizations adapted from (ENISA, 2012)

2.8 Information Security Management Systems (ISMS)

Information Security Management Systems (ISMS) is a systematic and structured approach to managing information so that it remains secure. ISMS implementation includes policies, processes, procedures, organizational structures and software and hardware functions. The ISMS implementation should be directly influenced by the organization's objectives, security requirements, processes employed, size and structure.

2.8.1 Why ISMS is needed?

Need for information security is increased from time to time with the broadening of communication in different ways. It is not possible to secure information with just using of technical countermeasures. According Karamanlis (2016), Risks associated with an organization's information asset need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated

with all forms of information within or used by the organization. The adoption of an ISMS is expected to be strategic decisions for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization. The design and implementation of an organization's ISMS is influenced by the need and objectives of the organizations, security requirements, the business processes employed and the size and structures of the organization.

2.8.2 ISO/IEC 27000 Standard Family

One of the well-known and well-used ISMS is the ISO 27000-series, which among other things offer best-practice recommendations for initiating, implementing and maintaining ISMS. The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001) and certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001. Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control-related guidelines as well as sector-specific guidance.

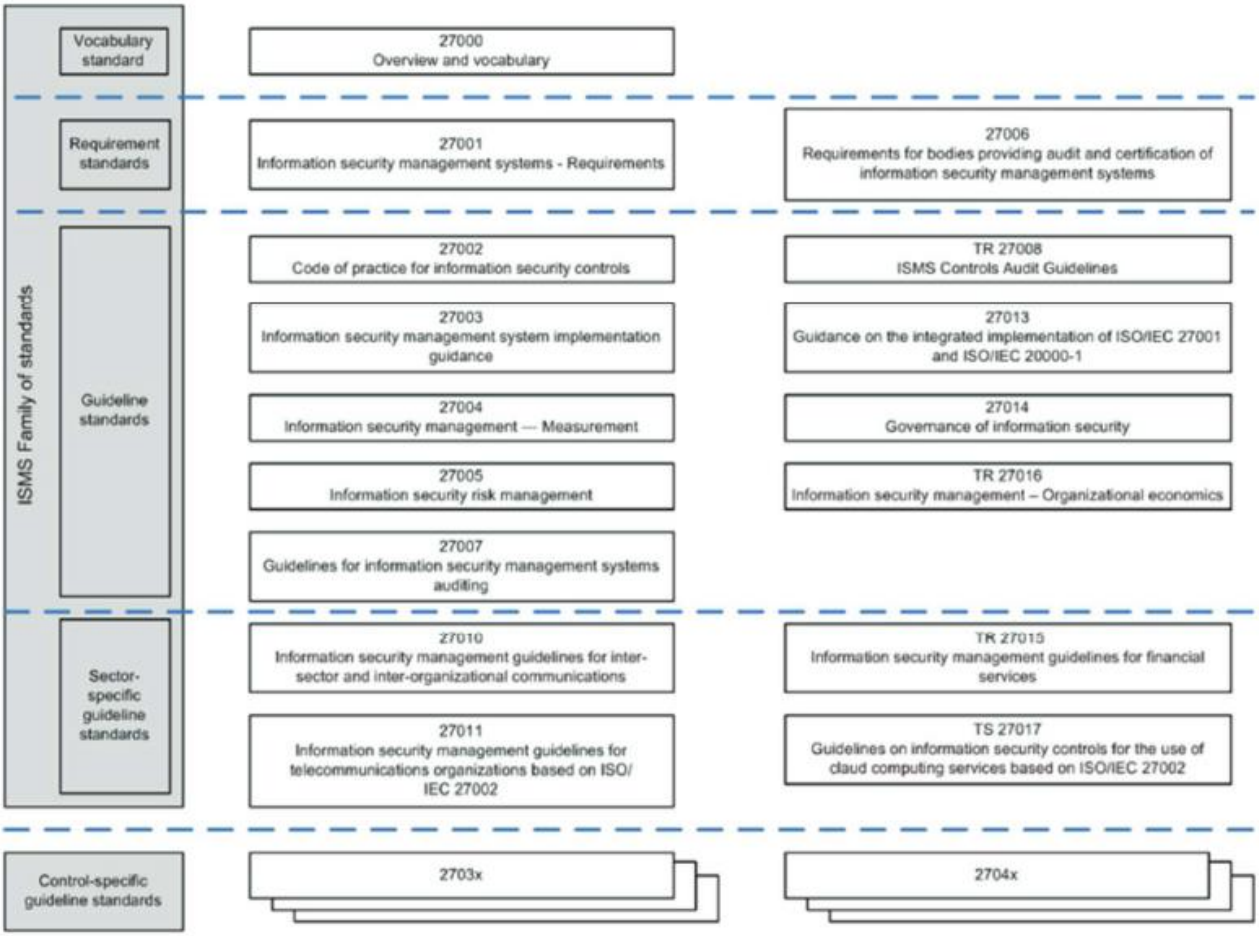

Figure 2.3: Relationships between ISMS families, adapted from (Karamanlis, 2016)

As we can see on the above table, the applicable clauses are:

1. Standards describing an overview and terminology
2. Standards specifying requirements
3. Standards describing general guidelines
4. Standards describing sector-specific guidelines

According Karamanlis (2016), all kind of organizations has identified and admitted that Information Security can improve the profitability of the company. List of ISO/IEC 27000-series information security standards which are published or currently being developed attached with APPENDIX C.

2.8.3 ISO/IEC 27001

Protection of information assets, mitigation of possible risks and continuity of business processes can be accomplished by implementing an ISMS with management support. ISMS is a management system anticipated by ISO 27001. Due to standard, all management systems related to information security are made to get management in direction of information security. ISMS includes the company structure, planning activities, company policies and responsibilities, applications, processes, procedures and resources. ISO 27001 standard document is used for accomplishing enterprise information security. It is also developed to be applicable to organizations of every size. It does not just deal with technical system security but overall information security.

ISO 27001 standard is prepared for implementing, realizing, operating, reviewing, continuing, and enhancing the Information Security Management System as a model. It is a strategic decision for a company to internalize the ISMS. The ISMS concept and execution of a company is affected by the needs of the organization, security prerequisite's, processes used, the structure, goals and the size of the business. Change in those factors and supportive systems is expected in time. Also an ISMS is expected to scale due to changing needs of a company. ISO 27001 is a process based standard. Every activity for having an output from an input is considered as a process. ISO 27001 has the following processes:

a. Understanding need for business information security and understanding the need for information security policy.
b. Having controls for managing risks of information security in managing overall risks for company.
c. Inspecting the performance of management system and reviewing the performance as well as its utility, when necessary.
d. Regular enhancement of management system based on measurement of key performance indicator's (KPI).

2.8.3.1 History of ISO/IEC 27001

ISO27k originated in the 1980s and continues to grow and change, reflecting ongoing evolution in the field, new challenges (such as cloud computing) and emerging consensus on good information security practices. ISO/IEC 27001 is derived from BS 7799 Part 2, first published as such by the

British Standards Institute in 1999. BS 7799 Part 2 was revised in 2002, explicitly incorporating the Deming-style Plan-Do-Check-Act cycle. BS 7799 part 2 was adopted as ISO/IEC 27001 in 2005 with various changes to reflect its new custodians.

These were the key stages in the development of the core standards.

Figure 2.4: Timeline of ISO27000 Series

2.8.3.2 Revision of ISO/IEC 27001:2005 to ISO/IEC 27001:2013

Due to the huge changes to the ecosystem which organizations are developed, generated the need of a revision of the old ISO/IEC 27001:2005 to the new ISO/IEC 27001:2013. The generic changes are that the new standard puts more emphasis on measuring and evaluating how well an organization's ISMS is performing. With the 2013 edition, there are some slight differences made to the standard itself. Some controls have changed and some merged together. Terms and definitions part is deprecated in 2013 edition. ISO 27001 edition of Terms and Definitions refer to ISO/IEC 27000 standard. Most important change in standard is there is no need for PDCA 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.

Do: the implementation and operation of the planned processes.

Check: the monitoring, measuring, evaluation, and review of results against the information security policy and objectives, so corrective and/or improvement actions can be determined and authorized.

Act: the performing of authorized actions to ensure the information security delivers its results and can be improved.

Tight relations 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 (Kosutic, 2014). Sections in 2013 edition can be matched with PDCA cycle steps as listed in figure 2.5.

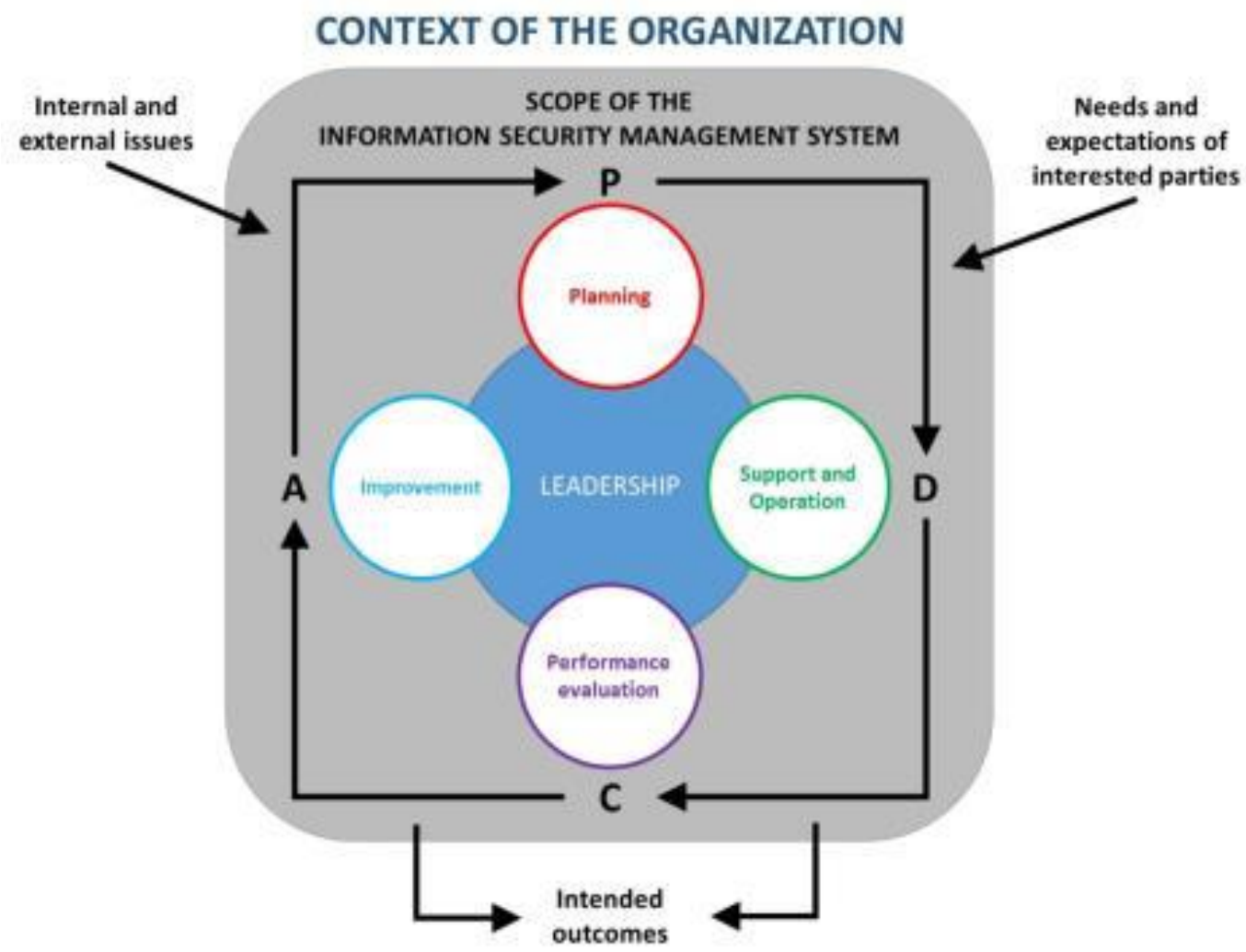

Figure 2-5: PDCA Cycle for ISMS processes; adapted from (Advisera, 2016).

Risk management section is aligned with the ISO 31000 standard. There is a new concept of Risk Owner and the management of risks has higher focus then the control effectiveness. Also there is no need for identifying assets, threats and vulnerabilities before risk identification. With the alignment of ISO 31000; risk management section now discusses consequences instead of impact.

Preventive action in risk management no longer exists but is replaced by "Risks and Opportunities". Also determination of controls is now a part of risk assessment instead of Annex A. But the need for validating selected controls from Annex A exists.

Requirements of an ISMS is revised in technical and structured manner. Standard clauses in 4-8 sections of 2005 edition is revised and improved as a new framework. New clauses listed in sections 4 – 10 is listed below.

Context of the Organization (Clause 4): - understanding the organizational context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 states very plainly that "The organization shall establish, implement, maintain and continually improve" the ISMS.

Leadership (Clause 5): - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.

Planning (Clause 6): - outlines the process to identify, analyze and plan to treat information risks, and clarify the objectives of information security.

Support (Clause 7): - includes preparing supportive and collateral resources for ISMS implementation, preparing for end user abilities and awareness, trainings, fulfillment of documentation needs and communicating with involved parties.

Operation (Clause 8): a bit more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).

Performance Evaluation (Clause 9): - monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary.

Improvement (Clause 10): - address the findings of audits and reviews (*e.g.* nonconformities and corrective actions), make continuous improvement on ISMS.

Total of 133 controls were listed in Annex – A of 2005 edition decreased to 114 controls in 2013 edition. Every risk has an owner in 2013 edition. Asset owner concept in 2005 edition is revised

as the risk owner. Risk owner will be responsible for risk mitigation plan and acceptance of risks. Risk management documentation is not necessary in 2013 edition but the process of risk management should be defined.

ISO/IEC 27001:2005 edition had five mandatory procedures but ISO/IEC 27001:2013 edition has removed the explicit requirement. Although there is still a requirement for documenting controls including supporting records. Internal audit is still required but it no longer requires a formal procedure. Management review no longer defines specific precise inputs and outputs but provides a list of topics that needs to be considered and must occur at planned intervals. At least annually.

2.8.4 ISO/IEC 27002:2013

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 must assess their own information risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.

The standard is structured logically around groups of related security controls. Many controls could have been put in several sections but, to avoid duplication and conflict, they were arbitrarily assigned to one and, in some cases, cross-referenced from elsewhere. This has resulted in a few oddities (such as section 6.2 on mobile devices and teleworking being part of section 6 on the organization of information security) but it is at least a reasonably comprehensive structure. It may not be perfect but it is good enough on the whole. Those new controls and sections in 2013 revision are listed in the attached Appendix D.

2.8.5 Benefits of implementing ISO/IEC 27001:2013 in Telecommunication

This standard delivers an application of Information Security Management within the telecom industry to ensure the confidentiality, integrity, and readiness of telecommunication services. The main benefits are:

- ✓ Providing Telecom operators with general security control objectives that are based on ISO/IEC 27002, leading to higher and safer levels of information security used inside the organization
- ✓ Telecommunication industry will have an increased level of reliance, which will generate higher business profits
- ✓ Discretion, reliability, and availability would be assured in Telecom organizations
- ✓ Adopting processes and controls that are secure and collaborative, which makes certain that the level of risks is lowered in terms of providing Telecom services
- ✓ Increased level of personal alertness as well as public confidence
- ✓ Implementing a continual and complete methodology for information technology.

2.9 Related works

To the best of the researcher's knowledge there is no obtainable work which identify the critical and mandatory requirements of ISM based on ISO/IEC 27001:2013 standard and best practices for ISM in Ethio telecom. Nevertheless, there are several works that are highly related to this academic work. Some of them are summarized briefly reviewed in the table below.

Author (year)	**Objectives**	**Methods/approach**	**Key finding**
İzzet Atıl Gürcan (2014)	Assessing information management requirements for finance sector using an ISO 27001 based approach	Surveying technique (Assessment)	Finance sector in turkey recognize their maturity level and find their strengths and weaknesses on ISO 27001:2013 certification and recommendation based on these results.
Al-Ahmad, W., & Mohammad, B. (2013)	Addressing Information Security Risks by Adopting Standards	Case study	Propose Model for Framework Selection
Yves Barlette and Vladislav V. Fomin (2009)	The adoption of Information Security Management Standards	Literature review	Provide recommendations on how to successfully implement and stimulate diffusion of information security standards in the

			dynamic business market environment
Kelemie Tebkew (2013)	To propose and develop ISM Framework which will work in banking industry in Ethiopia.	Case study	Developed information security management framework for the bank
Susanto (2011)	To set of benchmarks or standards to ensure the best security practices	Introduce various information security standards	The study provides a picture of the position and specialization of each standard usability levels.
Abeselom Negussie (2015)	Practices, Challenges and Prospects of Information Security Policy in Ethiopian Banking Industry	Surveying technique	Identified the security enhancement techniques.
Munir and Manarvi (2010)	Assessing Security risk for banking sector-A Case study of Pakistani Banks	Quantitative risk assessment(questionnaire)	Risk assessment is recommended to all assets in the organization.
Daniel Gebrehawariat (2017)	Assessment of the Effectiveness of Card Banking Security in the Ethiopian Financial Sector	Case study	Propose A Conceptual Framework for Card Banking Security
Nakrem, A. (2007).	Managing information security in organizations A CASE study	Case study	Propose A framework of information security handling

Table 2.3 Related works

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

INTRODUCTION

The previous chapter extensively reviewed the relevant literature. By doing so, it provided a theoretical and empirical background for the survey. This chapter aims to provide an overview of the research approaches used within the information security discipline that leads to the selection of proper research methodology for directing the justification of the conceptual framework, and thus answering the research question that the researcher used to analyze the current practices of ISM in Ethio telecom. In the following section, 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 and justified. Moreover, arguments for the validity and reliability of the work is given.

3.1 Research Methodology

A research methodology is a systematic approach to study a research problem from the theoretical underpinning of the research to the collection, analysis and interpretation of the data (Kothari 2007). It guides the research towards achieving its objectives (Creswell et al. 2011). The research methodology includes a variety of research methods that can be used for collecting, analyzing, and interpreting the data, and determining which specific research methods are appropriate and how these methods can be used for adequately answering the research questions (Creswell et al. 2011). Selecting an appropriate research methodology in a research project greatly depends on the nature of the research. This research aims to identify the critical and mandatory requirements for ISM based on ISO/IEC270001:2013 standard for Ethio telecom approach. The nature of this research is characterized in its pursuit of identifying the critical control for determining the information security management in the organization and the appropriate framework.

3.2 Research design

A research design is a plan used as a guide in collecting and analyzing research data for the study to be conducted. It describes the methods used to collect and analyze the data that helps to answer the research question. Research design is a blue print or guidance of the research (Kothari, 2007). Some scholars design their research in the following order: Literature review ➔ Case study or Assessing ➔ identify the critical and mandatory requirements of ISM for Ethio telecom.The researcher prefer this research design to reach sound and applicable requirements of ISM. In other words, to answer the research question properly.

- ***Literature Review:*** This research starts with a literature review focusing on key concepts from the areas of information security management studies.
- ***Assessing the Current ISM Practice in the Organization.***
  A mixed research methods (Qualitative and Quantitative methods) was applied to assess the current ISM practice.
- ***Identify the critical and mandatory requirements****:* The requirements of ISM will be identified based on literature review findings and the assessment result of the current ISM practice.
- ***Evaluating the requirements of ISM:*** The identified requirements of ISM will be evaluated by professionals (domain experts) and refined based on the sound comments and suggestions.

3.2.1 Main steps that are taken during this study

1. Conducting a literature review to capture ISM concepts
2. Assessing the current ISM practice and challenges
3. Analyzing collected data
4. Discussing the findings that result in from the data analysis with respect to the research questions.
5. Interpreting the findings against the context of the research framework (ISO 27001:2013)
6. Identify the critical and mandatory requirements of ISM based on the findings and assessment result.

7. Evaluating the requirements of ISM by domain experts.

8. Incorporate the sound feedback to Identify ISM requirements.

9. Concluding the thesis with a summary of the findings, the identified requirements of ISM and recommendations on how to implement the requirements.

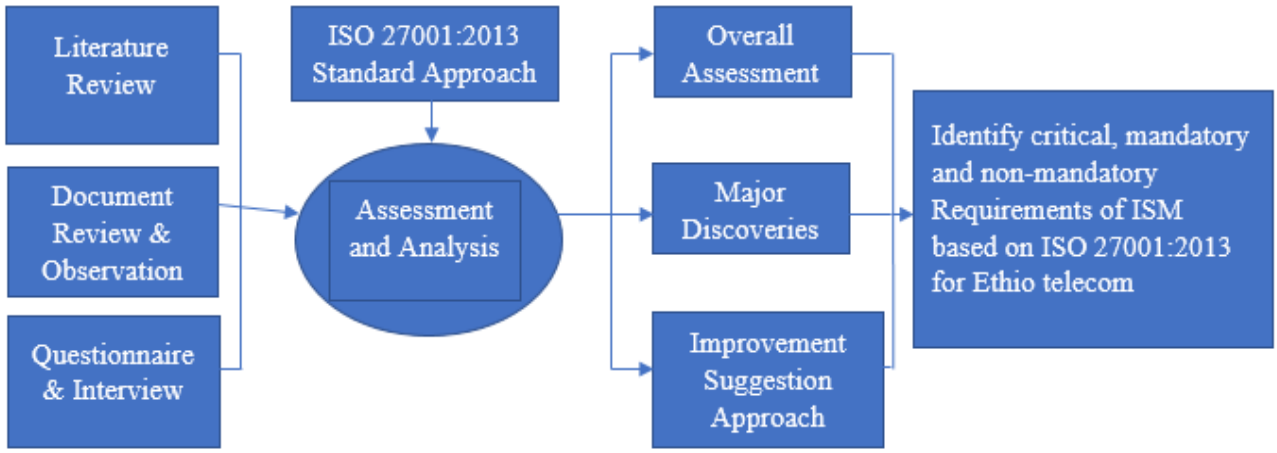

Figure 3.1. The research design and steps

3.3 Case Study Research Method

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 phenomenon 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. The case study research can be designed as either single or multiple cases (Yin, 2009). This research employed single case industry, Ethio telecom, which is a good exemplary as an IT industry, since it is the sole telecom service provider in the country. A single case is often selected because the case under study is both an exemplary case containing extreme and/or unique circumstances (Yin, 2009).

The study will be conducted using survey questionnaire, document analysis, and interview as a method of data collection and mixed research method as a research paradigm. The popularity of the mixed-methods methodology is due to the limitations associated with the use of quantitative and qualitative methodologies in research. A quantitative methodology, for example, is often

criticized for under-representing the context in which people talk (Creswell et al. 2011). A qualitative methodology, however, is often condemned due to the influence of individual researchers' biases and personal interpretations on people's voice. In contrast, a quantitative methodology is free of personal biases and interpretations. Furthermore, a quantitative methodology is credited for its ability to generalize findings to a large group. On the other hand, the findings from the use of a qualitative methodology cannot be generalized to a large group due to its small sample.

The capability of a mixed-methods methodology capitalizes on the strength of both quantitative and qualitative methodologies by combing both of them into a single study. The adoption of a mixed-methods methodology involves both quantitative data analysis techniques such as statistical analysis and qualitative data analysis techniques such as thematic analysis for answering the research question (Creswell et al. 2011). Therefore, the adoption of such a methodology is compatible with the selected paradigm and suitable for the stated purpose of the study. It is also relevant to gather detail description of existing condition and practices of ISM in Ethio telecom.

3.4 Source of Data

Regarding the research data of the study, as a primary data, questionnaire was used to collect information from the target group of Ethio telecom's information system division. 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, telecom's requirement, etc. In addition, secondary sources of data such as relevant best practices in information security policy, standard and procedure documents were used.

3.5 Sampling Design and Sampling Techniques

In conducting the quantitative research, designing a sample that reflects the theoretical population is critical for obtaining participants' responses to the developed questionnaire (Bell & Bryman 2007; Kotrlik & Higgins 2001). It requires substantial data from a representative proportion of the population for the conducted research. Since Ethio telecom is large and has wide area coverage all

over the country, participants for this survey are employees in information system division in Corporate Branch at head quarter. The survey questionnaires are prepared in English language.

3.5.1 Population

The population sample for this study is the employees in information system division (203) at Ethio telecom in Addis Ababa.

3.5.2 Sampling Method

The sampling method was purposive. According to Lisa (2008), purposive sampling is virtually synonymous with qualitative research and it is about defining the population of eligible data sources, prior to selecting the actual sample. In essence, determining which data sources met the goal of purposive sampling for a qualitative study is equivalent to defining a set of eligibility requirements for the population. Besides, 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. From a target population of 203 employees; three management members from the sample interviewed and 93 were invited to participate to respond for questionnaire.

3.5.3 Sample Scope

Sampling scope refers to a list or set of direction that identifies the target population. Thus, the target population of this study is the employees of Ethio telecom in information system division (ISD) which has a target population of 203.

3.5.4 Sample Size

The sample size of this study is 93 employee. This means 45% of the total population ((93/203)*100%).

3.6 Data Collection Methods

Generally, three types of instruments, namely: questionnaire, interview, Document analysis and observation were employed for the data collection. The primary data was collected through questionnaire and interview. Myers (2009) highlights that triangulation of data from different sources increases the quality of data, and accordingly the accuracy of the findings.

3.6.1 Survey Questionnaire

Based on an extensive review of the existing information security management literature, and having understanding of the subject, 61 questionnaire items are developed from ISO 27001:2013 for capturing the intended ISM practice in Ethio telecom. Appendix A, shows the items adopted from the ISO 27001:2013. The questionnaire consists of four parts. The first part is used to collect the participant's background information such as years of experience, job title, education background and other demographic information. For the second part, the participants need to answer questions that are related to administrative, security Policy and standards for information security management practice in Ethio telecom. For the third part, related to physical and environmental security and finally, the participants need to answer questions that are related to technical and operational information security practices in the organization. The questionnaire items are closed on practices and status in information security aspects. For better result, the questionnaire were prepared and distributed to three group of respondents,

- IT and Network Security had 61 questions(All),
- Critical system owners had 42 questions and
- System users had 37 questions.

Based on the sample size identified, the survey is conducted using a survey. 93 questionnaires are distributed using emails, and in person. The set of questionnaires were distributed to the respondents by the researcher. Participants are encouraged to fill the questionnaire with the help of the section managers and researcher. After distributing the survey questionnaires to the respondents, a follow-up phone calls and emails were made until the end of April 2018. The data collection process was administrated by the researcher.

3.6.2 Interview

In this study, semi-structured interview is adopted for data collection, semi-structured interviews allowed to access the understandings and positions of the participants with respect to the activities and events that are happening or have already passed in relation to Information Security management. Myers (2009) identified, semi-structured interviews are valuable for "finding out people's motivations, and their rationale as to why they did certain things".

The purposive sampling technique is followed, which is highly recommended for qualitative case study research (Neuman, 2003), in order to identify key participants within the information system division. The purposive sample in this study consists of IT and Network security officer (member of top Management), Network Security Manager and IT and Network security project manager because they are directly involved in Ethio telecom information Security Management , that enable them to have a detailed understanding of the phenomena understudy. Sarantakos (2005) suggests, in purposive sampling "the researcher purposely choose subjects who, in their opinion, are relevant to the project".

The appointment was given to interviewees approximately three days before their scheduled interview date. All interviews were conducted face-to-face, in person, at the interviewees' site of business, which facilitated the consultation of relevant documents if the interviewee needed to check details or share related materials. Prior to the interviews, participants are notified of the objectives of the study. All interviews were conducted in Amharic and transcribed into English. The interviews varied in length from 30 to 40 minutes. The participants did not wish to be recorded on tape and didn't want to disclose their name. During the interview, notes are taken so that a complete and accurate record of the conversation can be obtained. As Patton (2002) suggests, no matter what the form of interviewing type used, and no matter how interview questions are worded, all is wasted unless the word of the interviewee are taken accurately.

3.6.3 Document and Observation Analysis

3.6.3.1 Observation

In this study, a participant observation technique is adopted as the researcher is an insider, observed various information Security events, complex interactions and actions between individuals from the Ethio telecom employees and the stakeholders, while working side-by-side on the network security section. In participant observation, the researcher is entirely involved and becomes a participant in the culture or the context being observed (Collis & Hussey, 2009).

3.6.3.2 Document Analysis

Regarding document analysis, the Ethio telecom information security policy and procedures which is to be carried out in the day to day activities to protect the organizational information from external and internal threat was reviewed to make sure that if it is prepared according to international standard (ISO 27001:2013) covering all the assets at the organizations premises. The document analysis was also made for the purpose of cross checking the validity of the response given on the questionnaires.

3.7 Pilot Testing

Even if questionnaire are adapted from the international standard, ISO/IEC 27001:2013. It is essential to make a pilot study to avoid misunderstanding in the questions and to make sure that no ambiguity and error on the questions so that the researcher would get accurate data from the target population. The questionnaire is pretested with the help of advisor and some information security practitioners in Ethio telecom. They all are encouraged to check all the aspect of the questionnaire such as question wording, question order, redundant questions, and missing questions. These experts are also asked to restate questions that are difficult to understand. Positive feedbacks are received from pretesting the questionnaire with suggestions for minor changes. This results in the revision of the questionnaire items in finalizing the questionnaire in this study.

3.8 Validity and Reliability

To measure the quality of the research, both reliability and validity were applied. Reliability is used to measure the consistency of the survey, whereas validity is used to measure the degree to which a scale or set of measures accurately represents the construct (Hair et al., 1998).

In this work, the following strategies are adopted in order to increase the study's validity and reliability and to decrease possible biases:

- Multiple methods survey (questionnaire, document analysis, and interview) for collecting the data of this research are used, which permit the researcher to achieve triangulation. Myers (2009) highlights that triangulation of data from different sources increases the quality of data, and accordingly the accuracy of the findings.
- The questionnaires were adapted from international information security management standards of ISO/IEC 27001:2013. After the questionnaires are adapted, modifications and adjustments were made on the formatting after discussing with the advisor. Moreover, pilot test was made by distributing the questionnaires to some IT and Network Security department employees and some modification was made based on their feedback.
- The initial drafts of each of the semi-structured interviews reports are emailed to the participants of Ethio telecom in order to verify them for accuracy and to review them for comments, amendment, and further feedback and clarification where necessary.

3.9 Data Analysis Technique

The research results were interpreted from the quantitative perspective of the research process that can generate effective outputs. Analysis for qualitative and quantitative result were done at the integration phase for its needed interpretations. For both qualitative and quantitate case processing is on its own phase independently. SPSS version 20, graphical presentation, tabular presentation were used to analyze the quantitative data.

CHAPTER FOUR

FINDING AND DISCUSTION

4.1 Overview

This chapter presents the finding of the study and discussed the result accordingly. Hence, the findings are categorized in to fourteen sections. This includes: Information Security Policies, Organization of Information Security, Human Resource Security , Asset Management, Access Control, Cryptography, Physical and Environmental Security, Operations Security, Communications Security, System acquisition, Development and Maintenance, Supplier Relationships, Information Security Incident Management, Information Security aspects of Business Continuity Management, Compliance.

To address this, first, Ninety three questionnaire distribution procedure had been completed. The data was collected and verified to discover if there are incomplete and inconsistent responses from the target respondent. Eighty nine of the respondents filled and returned the questionnaire and four of the respondents failed to return the questionnaire. This implies 95% of the questionnaires are returned and 89 of them used for this study. Following to the verification of the questionnaires, the collected data was analyzed using SPSS version 20 to explore the results for further discussion and recommendation based on the findings. On top of the questionnaire, observation technique and interviews were also used as an instrument to strengthen the information gathered from the target population of the selected division of the organization. Regarding the result presentation, frequency and percentage is used in the table form since a frequency table is one of the most basic tools for displaying descriptive statistics which make it much easier to view and understand the result of the data presentation. Finally identify the critical and mandatory requirements of ISM with detail explanation about its components.

4.2. Respondent Demographic Characteristics

The demographic data incorporates respondent information from information system division in Ethio telecom. The respondent information covered information such as employee's job position, gender, educational status and work experience.

4.2.1 Distribution of respondents by gender

The study establish the gender distribution of the respondents, from the study revealed that majority of the respondents as shown by 79.8% were males whereas 20.2% of the respondents were females.

Gender		
Gender	Frequency	Percent
Male	71	79.8
Female	18	20.2

Table 4.1 Distribution of respondents by gender

4.2.2 Distribution of respondents by Educational Status

The study considered educational background of the respondents as presented in the table 4.2. Majority of the respondents are bachelor degree holders with percentage of 79.8%. Whereas 16.9% of the respondents had master degree, Moreover, (3.4%) of the respondents refuse to indicate their educational status. More than 95% are bachelor degree and above holders. This implies that respondents were well educated and therefore they were in position to respond to the research question with ease.

Educational Status		
Educational Status	Frequency	Percent
Diploma	0	0.0
Degree	71	79.8
Masters	15	16.9
Missing	4	3.4
PhD	0	0.0
Total	89	100.0

Table 4.2 Distribution of respondents by Educational Status

4.2.3 Distribution of respondents by Job Position

With regard to the job position of the respondents (Table 4.3) shows that 9(10.1%) of the respondents are Network Security Specialist, 11 (12.4%) are in a position IT Security Specialist, 6(6.7%) are in a position Security Operation Center Specialist,6(6.7%) are in a position Fraud Management System Specialist,10 (11.2%) are in a position IT Technical Operation Specialist, 9(10.1%) are in a position Corporate Application Administrator, 11(12.4%) are in a position

Business Application Administrator,8(9.0%) are in a position IT Service Desk Specialist, 6(6.7%) are in a position System Administrator, and 13(14.6%) are in a position IT Solution Engineer.

Job Position		
Job position	Frequency	Percent (%)
Network Security Specialist	9	10.1
IT Security Specialist	11	12.4
Security Operation Center Specialist	6	6.7
Fraud Management System Specialist	6	6.7
IT Technical Operation Specialist	10	11.2
Corporate Application Administrator	9	10.1
Business Application Administrator	11	12.4
IT Service Desk Specialist	8	9.0
System Administrator	6	6.7
IT Solution Engineer	13	14.6
Total	89	100.0

Table 4.3 Distribution of respondents by Job Title

4.2.4 Distribution of respondents by work experience

When we see the respondent by their work experience (table 4.4) 24 (27.0%) respondents are categorized under the work experience range 1-5 Years, 31(34.8) % of the respondents are found in the age range of 6-10 years. 18(20.2) % of the respondents are found in the age range of 11-15 years. 14 (15.7%) are under the work experience range above 15 years,. Only 2 (2.2 %) respondents refuse to indicate their work experience which considered as a missing value.

Work Experience		
	Frequency	Percent
1-5 Years	24	27.0
6-10 Years	31	34.8
11-15 Years	18	20.2
Above 15 Years	14	15.7
Missing Value	2	2.2
Total	89	100.0

Table 4.4 Distribution of respondents by work experience

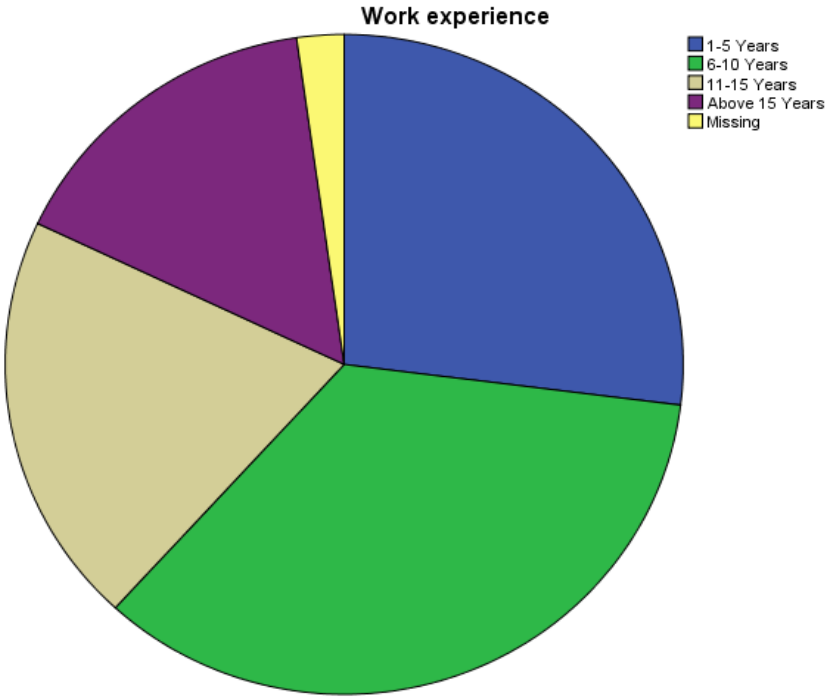

Figure 4-1: Distribution of respondents by work experience

4.3 Quantitative Data Analysis and Presentation

The "Yes", "Partial", "No", "I don't know" options were used to identify the level of the independent variable practiced by the Ethio telecom Information system division and encoding the questionnaire. The four options are used to indicate the capability level of the Ethio telecom information security management practices fully practiced, rarely, completely not practiced or don't have information about items in the ISO/IEC 27001:2013. The following table clarifies the options.

Options Clarification	
Options	**Meaning**
Yes	The organization is performed or practiced it fully
Partial	Incomplete and not fully exercised in the organization
No	The organization is completely not practiced it fully
I don't know	Does not have the information in the organization

Table 4.5 Clarification of Options

4.3.1 Practices of Information Security Policies

To understand about the availability and practice of the information security policies, five questions provided that comprises of having security policy and approved by management, if it is communicated to employees, reviewed and updated periodically. In addition, whether it reviews conducted when circumstances change. Thus, the summarized result of the collected information regarding the information security policies is as below in table 4.6. Regarding the summarized result of ISP, 28.92% of the respondents agree that the organization is has information security policies , 33.34% of the respondents indicate that incomplete or partial information security policies exist in the organization, 26.76% respondents the organization doesn't have ISP and 10.98% of the respondents don't have information about the ISP whether it is owned or not. However, 19.3% respondents indicate that the existing security policy communicated to employees, whereas, 44.3% respondents responded partially communicated, 21.2% not communicated and 15.2% respondents don't know whether it is communicated or not.

S.N	Items under Information security policies (ISP)	Yes	Partially	No	I don't Know
1	Have security policy and approved by management (1)	53 59.6%	25 28.1%	2 2.2%	9 10.1%
2	ISP communicated to employees (2)	17 19.3%	39 44.3%	26 29.5%	6 6.8%
3	ISP reviewed and updated periodically (3)	6 18.2%	15 45.5%	7 21.2%	5 15.2%
4	Reviews conducted when circumstances change (4)	2 6.9%	6 20.7%	18 62.1%	3 10.3%

S.N	Items under Information security policies (ISP)	Yes	Partially	No	I don't Know
5	Roles, responsibilities, and authorities for IS assigned (12)	13 40.6%	9 28.1%	6 18.8%	4 12.5%
	Total Score	**28.92%**	**33.34%**	**26.76%**	**10.98%**

Table 4.6 Practices of Information Security Policies

4.3.2 Practices of Organization of Information Security

There are ten items that asked about the availability and practice of organizational information security of the organization. Thus, the summarized result of the collected information regarding the organization of information security stated below in table 4.7.Regarding the summarized result of OIS 42.55% of the respondents agree that the organization identify and define the organizational information security, 29.73% of the respondents indicates incomplete or partial. However, 14.09% of the respondents indicates that there is no organizational information security in place. Contrarily, 65.2% of the respondents partially believe that management support for OIS is weak.

S.N	Items under Organization of information security (OIS)	Yes	Partially	No	I don't Know
1	Has contacts with authorities & special interest groups (7)	7 21.9%	7 21.9%	9 28.1%	9 28.1%
2	Use industry standards or frameworks (8)	10 37.0%	8 29.6%	4 14.8%	5 18.5%
3	Lack of experienced staff on international Standards, lack of local ISMF and budget (11)	20	7	1	5

S. N	Items under Organization of information security (OIS)	Yes	Partially	No	I don't Know
		60.6%	21.2%	3.0%	15.2%
4	Management Support (14)	6 6.7%	58 65.2%	25 28.1%	0 0%
5	Separating Security team from IT functional team (16)	52 58.4%	14 15.7%	14 15.7%	9 10.1%
6	Have duties and areas of responsibility separated (17)	47 52.8%	28 31.5%	7 7.9%	7 7.9%
7	Projects go through information security assessment (18)	11 19.3%	29 50.9%	8 14.0%	9 15.8%
8	Has secure handling of mobile devices (19)	22 25.0%	35 39.8%	12 13.6%	19 21.6%
9	Use wireless technology (52)	70 80.5%	10 11.5%	5 5.7%	2 2.3%
10	Employed WEP and WPA technologies (53)	38 63.3%	6 10.0%	6 10.0%	10 16.7%
	Total Score	**42.55%**	**29.73%**	**14.09%**	**13.62%**

Table 4.7 Practices of Organization of Information Security

4.3.3 Practices of Human Resource Security

There are three items that asked about the human resource security of the organization. Thus, As the summarized result shows, 19.33% of the humane security practice is secured, 41.30% of the humane security is partially secured, 24.63% of the humane security is not secured, whereas the rest 14.77% don't know if it is secured or not in the organizations. Similarly, 2.3% respondents believe that staffs have awareness on emerging technologies, 71.6% partially agreed, 23.9% totally disagree and the rest 2.3% don't have information about it.

S. N	Items under Human resource security (HRS)	Yes	Partially	No	I don't Know
1	Employees have written job description including IS responsibility (25)	24 27.3%	28 31.8%	22 25.0%	14 15.9%
2	employees and contractors sign confidentiality or non-disclosure agreement (27)	25 28.4%	18 20.5%	22 25.0%	23 26.1%
3	technical staff awareness about emerging technologies (30)	2 2.3%	63 71.6%	21 23.9%	2 2.3%
	Total Score	**19.33%**	**41.30%**	**24.63%**	**14.77%**

Table 4.8 Practices of Human Resource Security

4.3.4 Practices of Asset Management

Under asset management there are three items as shown in table 4.9. The summarized result shows that 20.93% respondents answered YES on having asset management in practice, 38.80% partially agreed, 18.27% responded don't have this practice, whereas 22.07% are don't know if there is asset management in place. Especially, 25.0% respondents know that assets have clearly defined owner, 48.9% respondents agree partially on this practice, 14.8% of the respondents not practiced, the rest 11.4% don't have the information.

S. N	Items under Asset management (AM)	Yes	Partially	No	I don't Know
1	Have information asset inventory & classification scheme (22)	20 23.0%	35 40.2%	14 16.1%	18 20.7%
2	Assets have a clearly defined owner (23)	22 25.0%	43 48.9%	13 14.8%	10 11.4%
3	Has procedure on how removable media transported and disposed (24)	13 14.8%	24 27.3%	21 23.9%	30 34.1%
	Total Score	**20.93%**	**38.80%**	**18.27%**	**22.07%**

Table 4.9 Practices of Asset Management

4.3.5 Practices of Access Control

To understand about the availability and practice of the access control, eleven questions provided that comprises of having access control or not. Thus, the summarized result of the collected information regarding the access control is as below in table 4.10. Regarding the summarized result of access control, 49.07% of the respondents agree that the organization is has access control practices, 26.20% of the respondents indicate that incomplete or partial access control activities exist in the organization, 6.34% respondents the organization doesn't have access control and 18.37% of the respondents don't have information about the access control whether it is practiced or not.

S. N	Items under Access control (AC)	Yes	Partially	No	I don't Know
1	Has disable default username and passwords(41a)	42 48.8%	21 24.4%	5 5.8%	18 20.9%
2	Only authorized user accessed the resources(41b)	48 55.8%	29 33.7%	2 2.3%	7 8.1%
3	Disabled or closed unnecessary protocol, services and ports (41c)	37 43.0%	32 37.2%	5 5.8%	12 14.0%
4	Has user access control policy (44)	37 44.6%	31 37.3%	5 6.0%	10 12.0%
5	Reviewing user access rights (45)	38 44.2%	32 37.2%	12 14.0%	4 4.7%
6	Has user registration and de-registration procedures (46)	14 22.2%	17 27.0%	10 15.9%	22 34.9%
7	Has password guidelines (47)	52 60.5%	28 32.6%	3 3.5%	3 3.5%
8	Has internal firewall between intranet and DMZ (48)	21 67.7%	4 12.9%	0 0%	6 19.4%
9	Has external firewall between DMZ and internet (49)	19 61.3%	2 6.5%	1 3.2%	9 29.0%

10	Use different vendors firewall (50)	13 43.3%	7 23.3%	3 10.0%	7 23.3%
11	Implement Access control system (51)	15 48.4%	5 16.1%	1 3.2%	10 32.3%
	Total Score	**49.07%**	**26.20%**	**6.34%**	**18.37%**

Table 4.10 Practices of Access control

4.3.6 Practices of Cryptography

S. N	Items under Cryptography (C)	Yes	Partially	No	I don't Know
1	have authentication mechanism for challenging external connections (60)	12 40%	8 26.7%	1 3.3%	9 30.0%
2	Use Cryptography (60a)	8 44.4%	5 27.8%	0 0%	5 27.8%
3	Employed hardware or software tokens(60b)	5 31.5%	5 31.5%	0 0%	6 37.5%
	Total Score	**38.633%**	**28.667%**	**1.100%**	**31.767%**

Table 4.11 Practices of Cryptography

4.3.7 Practices of Physical and Environmental Security

Under physical and environmental security there are eight items as shown in table 4.12. The summarized result shows that 66.35% respondents answered YES on having physical and environmental security in practice, 20.86% partially agreed, 3.96% responded don't have this

practice, whereas 8.83% are don't know if there is physical and environmental security in place. Especially, 43% respondents know that visitors and contractors are supervised, 25.6% respondents agree partially on this practice, 11.6% of the respondents not practiced, the rest 19.8% don't have the information.

S. N	Items under Physical and Environmental Security (PES)	Yes	Partially	No	I don't Know
1	Has alternate power source (35a)	72 85.7%	11 13.1%	0 0%	1 1.2%
2	Has air conditioning (35b)	70 82.4%	11 12.9%	1 1.2%	3 3.5%
3	Has fire suppression and water leakage (35c)	51 59.3%	24 27.9%	2 2.3%	9 10.5%
4	Has fence and/or human security guards (35d)	64 76.2%	12 14.3%	2 2.4%	6 7.1%
5	Has Door Access cards & CCTV (35e)	59 69.4%	21 24.7%	2 2.4%	3 3.5%
6	perimeter security controls defined (36)	47 56.0%	16 19.0%	6 7.1%	15 17.9%
7	Visitors and contractors are supervised (37)	37 43%	22 25.6%	10 11.6%	17 19.8%
8	Performing equipment authorization and checking (38)	50	25	4	6

S. N	Items under Physical and Environmental Security (PES)	Yes	Partially	No	I don't Know
		58.8%	29.4%	4.7%	7.1%
	Total Score	**66.35%**	**20.86%**	**3.96%**	**8.83%**

Table 4.12 Practices of Physical and environmental security

4.3.8 Practices of Operations Security

There are nine items that asked about the operations security of the organization. Thus, the summarized result of the collected information regarding the operations security stated below in table 4.13. 46.41% respondents respond "YES" that the operations security practiced very well, 30.72% partially practiced, whereas 8.11% are neutral 14.77% respondents don't have if the operational security activities applied or not. Whereas 30.6% the respondents have a practice of a well documents of operating procedures, 40.0% partially practiced, 16.5% respondents don't have such documents and 12.9% of respondents don't have information about it.

S. N	Items under Operations security (OS)	Yes	Partially	No	I don't Know
1	Perform patch management (39)	6 20.0%	11 36.7%	6 20.0%	7 23.3%
2	Log Monitoring (40)	22 51.2%	18 41.9%	1 2.3%	2 4.7%
3	Has controlled change management process (42)	52 59.1%	20 22.7%	1 1.1%	15 17.0%

S. N	Items under Operations security (OS)	Yes	Partially	No	I don't Know
4	Antivirus installed and regularly updated (54)	60 69.8%	22 25.6%	3 3.5%	1 1.2%
5	Use firewall and web security (55)	20 64.5%	7 22.6%	0 0%	4 12.9%
6	Operating procedures well documented (56)	26 30.6%	34 40.0%	14 16.5%	11 12.9%
7	Taking regular backup (57)	34 39.1%	26 29.9%	7 8.0%	20 23.0%
8	Separating internet and data line (58)	42 48.8%	16 18.6%	7 8.1%	21 24.4%
9	Has synchronized clock in all IT systems (59)	18 34.6%	20 38.5%	7 13.5%	7 13.5%
	Total Score	**46.41%**	**30.72%**	**8.11%**	**14.77%**

Table 4.13 Practices of Operations security

4.3.9 Practice of Communications security

As the summarized result shows, 20.13% of the respondents the communications security is secured, 21.97% of the respondents the communications security is partially secured, 34.30% of the respondents the communications security is not secured, 23.60% of the respondents don't know have information about communications security. Whereas, 70% of the respondents result shows that there is no information security awareness for employee and third party.

S. N	Items under Communications security (CS)	Yes	Partially	No	I don't Know
1	Has annual budget for SAP and security technical training (15)	6 6.9%	17 19.5%	23 26.4%	41 47.1%
2	Employee and third party IS awareness frequency (29)	3 3.5%	16 18.6%	61 70.9%	6 7.0%
3	Perform network management process (43)	27 50.0%	15 27.8%	3 5.6%	9 16.7%
	Total Score	**20.13%**	**21.97%**	**34.30%**	**23.60%**

Table 4.14 Capability level of Communications security (Frequency and Percentage)

4.3.10 Practice of System Acquisition, Development and Maintenance

Under System acquisition, development and maintenance there are six items as shown in table 4.15. The summarized result shows that 20.62% respondents answered YES on having System acquisition, development and maintenance security in practice, 35.02% partially agreed, 27.02% responded don't have this practice, whereas 17.33% are don't know if there is System acquisition, development and maintenance in place. Especially, 9.1% respondents know that performing risk assessment, 42.4% respondents agree partially on this practice, 30.3% of the respondents not practiced, the rest 18.2% don't have the information.

S. N	Items under System acquisition, development and maintenance (SADM)	Yes	Partially	No	I don't Know
1	Security policy development involve stakeholders (5)	8	12	4	8

S. N	Items under System acquisition, development and maintenance (SADM)	Yes	Partially	No	I don't Know
		25.0%	37.5%	12.5%	25.0%
2	ISP consider all user have access to ET network (6)	32 36.8%	34 39.1%	12 13.8%	9 10.3%
3	Perform risk assessment (9)	3 9.1%	14 42.4%	10 30.3%	6 18.2%
4	Employees involvement in ISP development (26)	8 9.2%	23 26.4%	44 50.6%	12 13.8%
5	Perform periodical penetration testing (34)	5 17.2%	4 13.8%	11 37.9%	9 31.0%
6	Conducting security requirement before system development (61)	14 26.4%	27 50.9%	9 17.0%	3 5.7%
	Total Score	**20.62%**	**35.02%**	**27.02%**	**17.33%**

Table 4.15 Practices of System Acquisition, Development and Maintenance

4.3.11 Practices of Supplier Relationships

There are two items that asked about the Supplier relationships of the organization. Thus, the summarized result of the collected information regarding the organization of Supplier relationships security stated below in table 4.16. 16.50% respondents respond "YES" that the supplier relationships practiced very well, 44.40% partially practiced, whereas 6.75% are neutral 32.35% respondents don't have if the supplier relationships activities applied or not. Whereas 30.6% the

respondents the organization have a practice of identifying and controlling risks from third party, 40.0% partially practiced, 16.5% respondents don't have such documents and 12.9% of respondents don't have information about it.

S.N	Items under Supplier relationships (SR)	Yes	Partially	No	I don't Know
1	risks from third party identified and controlled (10)	3 9.4%	22 68.8%	2 6.3%	5 15.6%
2	supplier agreements include IS with in product supply chain (28)	13 23.6%	11 20.0%	4 7.3	27 49.1%
	Total Score	**16.50%**	**44.40%**	**6.75%**	**32.35%**

Table 4.16 Practices of Supplier Relationships

4.3.12 Practices of Information Security Incident Management

There is one item that asked about the information security incident management of the organization. Thus, the summarized result of the collected information regarding the information security incident management stated below in table 4.17. 39.8% respondents respond "YES" that the information security incident management practiced very well, 37.5% partially practiced, whereas 3.4% are neutral, 19.3% respondents don't have if the information security incident management activities applied or not.

S.N	Items under Information security incident management (ISIM)	Yes	Partially	No	I don't Know
1	Has incident management and formal reporting procedure (31)	35 39.8%	33 37.5%	3 3.4%	17 19.3%
	Total Score	**39.8%**	**37.5%**	**3.4%**	**19.3%**

Table 4.17 Practices of Information Security Incident Management

4.3.13 Practices of Information Security aspects of Business Continuity Management

To understand about the availability and practice of the information security aspects of business continuity management, two questions provided that comprises of having information security aspects of business continuity management or not. Thus, the summarized result of the collected information regarding the Information security aspects of business continuity management is as below in table 4.18. Regarding the summarized result of access control, 53.10% of the respondents agree that the organization is has information security aspects of business continuity management practices, 23.40% of the respondents indicate that incomplete or partial activities exist in the organization, 5.7% respondents the organization doesn't have this practice and 17.75% of the respondents don't have information about the information security aspects of business continuity management whether it is practiced or not.

S. N	Items under Information security aspects of business continuity management (ISBCM)	Yes	Partially	No	I don't Know
1	Has approved business continuity plan (32)	43 49.4%	18 20.7%	5 5.7%	21 24.1%
2	Has disaster recovery plan which is tested and exercised (33)	50	23	5	10

S. N	Items under Information security aspects of business continuity management (ISBCM)	Yes	Partially	No	I don't Know
		56.8%	26.1%	5.7%	11.4%
	Total Score	**53.10%**	**23.40%**	**5.70%**	**17.75%**

Table 4.18 Practices of Information Security aspects of Business Continuity Management

4.3.14 Practices of Compliance

To understand about the availability and practice of the compliance aspects of the organization, two questions provided that comprises of having compliance or not. Thus, the survey results below in table 4.18, shows that 7.90% respondents of the organization have compliance with the standard, 16.35% respondents is partially compliant, 51.40% respondents is not compliant and 24.45% of respondents don't have information about it.

S. N	Items under Compliance (CO)	Yes	Partially	No	I don't Know
1	Perform regular information system security audit (20)	7 12.7%	18 32.7%	17 30.9%	13 23.9%
2	Outsource IT systems security audit to third party (21)	1 3.1%	0 0%	23 71.9%	8 25.0%
	Total Score	**7.90%**	**16.35%**	**51.40%**	**24.45%**

Table 4.19 Practices of Compliance

4.3.15 Summarized Result of Practices with respect to ISO/IEC 27001:2013

Controls are all those countermeasures or safeguards that are put in place in the organizations and that make up the information security management system .As we can see from the summarized graphs Figure 4-2 below, in general specking Ethio telecom has weak information security practices with respect to the standard controls such having security policies & procedures, standard usage, Stakeholders involvement, risk assessment, management support, organizational and operational security, asset management, and staff awareness.

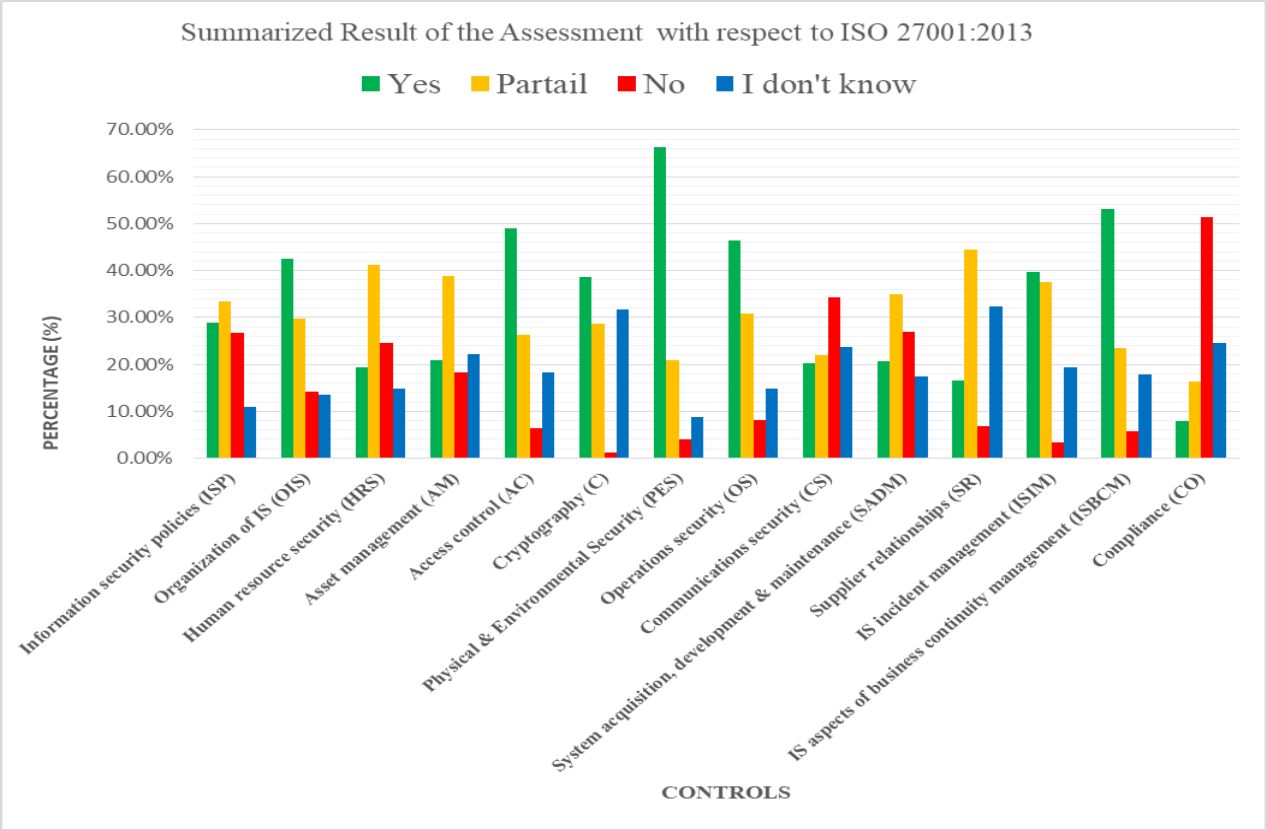

Figure 4-2: Summarized Result of Practices with respect to ISO/IEC 27001:2013

4.4 Qualitative Data Analysis

This analysis of qualitative data is done using thematic analysis. Interview findings are described in terms of words, and are structured as per the interview questions, as follows:

- ISM Framework that the organization has employed and its drawback(s) and strength(s)
- Issues concern most about the information security in Ethio telecom
- Methods of security requirement identification prior to select best practices

- Problems that impede and success factors in the process of development and implementation of ISMS
- A kind of risk management methodology that Ethio telecom have used
- Information security management structural organization

The aim of this analysis is to examine the different IT and Network security officer and managers view and idea regards to the management of information security in the organization. The interviewees hold, as well as to arrive at condensed descriptions of these views. The organization of this section is summarized and presented in the table 4.20 below. Then, a final synthesis is made that integrates these views under the questions.

Interview Questions	**Reponses**		
	Interviewee 01	***Interviewee 02***	***Interviewee 03***
Do you have developed ISMS in your organization? If you have, what kind of standard or framework the organization employed in the process of ISMS development? If not developed ISMS, what are the reasons?	*We did not develop ISMS we prepared proposal but it needs Board of Directors approval but not approved due to different reason.*	*No ISMS with a specific framework or standard is employed, the reason could be many reasons and one of those and the main one is lack of knowledge and experience to design the security posture of the company as needed.*	*ITIL*
If you developed ISMS in your company, what is/are the drawback(s) and strength of the standard that you have employed in ISMS development?	*Not, deploy*	*Not Applicable*	*There is no risk assessment and appropriate control selected.*

If you developed ISMS in your company, what is/are the drawback(s) and strength of the standard that you have employed in ISMS development?	*The first is issue responsibility of cyber security or information security should be owned by the top management/CEO and above position. And the process should be from top to bottom. If the tom management did not have the awareness of cyber security risk management it is difficult to implement the cyber security or information security governance and frameworks.*	*The most critical issues of my concern for Ethio Telecom regarding information security is that the company doesn't have a well-defined and designed security-architecture, governance, and framework which place the company in the competitive position with other international telecom service providers.*	*No clear list of assets and accordingly there is no defined threats for assets vulnerability.*
How the organization identifies its security requirements prior to selecting best practices or controls?	*from risk assessment and best practices and national and international information security standards*	*By conducting assessments, identifying the security gaps in the services and systems, and taking inputs from system owners of different sections.*	*Without any risk assessment just by brainstorming.*
What Requirements do you think are critical to the success of Ethio telecom's information security management? Please support your answers with justification.	*First cyber security governance should be in place this governance should be comply with national security and enterprise business process to meet the business needs.* *-Approved ISM policy* *-Budget*	*The most critical requirement for the success of the company for the same subject matter is that to work on commitment on the pillars of security which shape the security posture of the company, these are the security governance, security framework, and security architectures along with security compliance which are defined on those internationally accepted and tested standards, and practices.*	*Leadership or top management support. Employee Information Security Awareness*
From what aspects do you think Ethio telecom's information security management can be improved?	*From governance perspective and wariness creation perspective. Relatively technology is better but needs Up-to-date and continuous training for the professionals*	*The aspects which needs to be done with priority are the structures on which the security of the company will be built, and these structures are those dimensions mentioned above and which are the critical ones to be done to*	*Just assess the benefit of security frameworks and select one or more frame works and standards then implement security risk assessment based frame work or standard.*

		get the info sec management improved.	
What is your opinion about the pros and cons of separating Information security management team from other IT staffs structurally in IT department?	*Advantage: it has separate mission for more controlling purpose separation is better. For big organization separate management is better for check and balance. Disadvantage: knowledge less knowledge share if it is separate to monitor the security it needs to know the IT and network operational part also.*	*There will be no cons totally but pros only as per my opinion or the common practice what the world is following, the Info sec management needs to be structured separately as it manages all systems and service not only in the IT dept. but also those apart from IT.* Documented security processes	*Security and IT are different streams. And IT focuses all the IT and business alignment and running IT operations but security all the security and business alignment and security business data. As a result the IT manager focusses on the IT and security manager focusses on the security. So, separating Security helps to deliver balanced IT and Security values.*

Table 4.20 Summarized result of interview responses

4.5 Summary of the Interview findings

The results, presented in summary in table 4-20 indicate how the interviewed managers perceive and perform information security management in Ethio telecom. Focus is to arrive at an integrated view based on their perceptions and activities rather than trying to emphasize the differences among them.

- All Interviewees of the company explained that there is no formal and compressive developed ISMS in Ethio telecom. But according to one of the interviewees, there is initiation to assess the risk and develop information security that can cover all the services in premises.
- The main challenges in designing and implementation of ISMS project are:

- *Lack of top management understanding about ISMS designing and implementing ISMS, as result there is no ISMS designing and implementation.*
- *No inventory of assets and their potential risk*
- *There is no formal risk assessment*

- The summarized major success factors which are explained by the interviewees are:
  - *Firstly, having security governance with respect national security and business need.*
  - *Leadership or top management support/commitment*
  - *Having security framework with security compliance which are accepted and tested internationally.*
  - Budget

- Form the above three interviewees' explanation there is no predefined security requirement identification methodology or model methods of security requirement identification prior to select best practices. They just use :
  - *Brainstorming*
  - *Conducting assessments and taking inputs from system owners of different sections.*
  - *Trying referred best practices, national and international information security standards*

All interviewees have agreed on the point even though the real structure of the IT department is not structurally isolated. The structure /organization of IT department have a great contribution in information security management.

4.6 The identified ISM requirements and their importance status

This study advises Ethio telecom on how to protect their information and information systems against today's threats. As per the study of CESG (2015) on security procedures for telecommunications systems and services based on the ISO 27001:2013 is categorized as critical, mandatory and non-mandatory. Based on this study, experts comment and my personal experience in telecom security sector, out of the 114 controls 16 of them are critical, 72 of them are mandatory and 26 of them are non-mandatory by considering Ethio telecom context. The detail controls and clauses are summarized in the table 4.21.

REFERENCE STANDARDS	COMPLIANCE ASSESSMENT AREA (SECTION)	STATUS
A.5	**INFORMATION SECURITY POLICIES**	
A.5.1	**Management Direction For Information Security**	
A.5.1.1	Policies for information security	**Mandatory**
A.5.1.2	Review of the policies for information security	**Mandatory**
A.6	**ORGANIZATION OF INFORMATION SECURITY**	
A.6.1	**Internal Organization**	
A.6.1.1	Information security roles and responsibilities	**Critical**
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	**Mandatory**
A.6.2	**MOBILE DEVICE AND TELEWORKING**	
A.6.2.1	Mobile device policy	**Mandatory**
A.6.2.2	Teleworking	**Mandatory**
A.7	**HUMAN RESOURCES SECURITY**	
A.7.1	**PRIOR TO EMPLOYMENT**	
A.7.1.1	Screening	**Mandatory**
A.7.1.2	Terms and conditions of employment	**Mandatory**
A.7.2	**DURING EMPLOYMENT**	
A.7.2.1	Management responsibilities	**Mandatory**
A.7.2.2	Information security awareness, education and training	**Critical**

A.7.2.3	Disciplinary process	**Mandatory**
A.7.3	**TERMINATION AND CHANGE OF EMPLOYMENT**	
A.7.3.1	Termination or change of employment responsibilities	**Mandatory**
A.8	**ASSET MANAGEMENT**	
A.8.1	**RESPONSIBILITY FOR ASSETS**	
A.8.1.1	Inventory of assets	**Mandatory**
A.8.1.2	Ownership of assets	**Critical**
A.8.1.3	Acceptable use of assets	**Mandatory**
A.8.1.4	Return of assets	**Mandatory**
A.8.2	**INFORMATION CLASSIFICATION**	
A.8.2.1	Classification of information	**Mandatory**
A.8.2.2	Labelling of information	**Mandatory**
A.8.2.3	Handling of assets	**Mandatory**
A.8.3	**MEDIA HANDLING**	
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	**ACCESS CONTROL**	
A.9.1	**BUSINESS REQUIREMENTS FOR ACCESS CONTROL**	
A.9.1.1	Access control policy	**Critical**
A.9.1.2	Access to networks and network services	**Mandatory**
A.9.2	**USER ACCESS MANAGEMENT**	
A.9.2.1	User registration and de-registration	**Mandatory**

A.9.2.2	User access provisioning	**Mandatory**
A.9.2.3	Management of privileged access rights	**Critical**
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	**Critical**
A.9.3	**USER RESPONSIBILITIES**	
A.9.3.1	Use of secret authentication information	**Mandatory**
A.9.4	**SYSTEM AND APPLICATION ACCESS CONTROL**	
A.9.4.1	Information access restriction	**Mandatory**
A.9.4.2	Secure log-on procedures	**Mandatory**
A.9.4.3	Password management system	**Mandatory**
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	**CRYPTOGRAPHIC CONTROLS**	**Non-Mandatory**
A.10.1.1	Policy on the use of cryptographic controls	**Non-Mandatory**
A.10.1.2	Key management	**Non-Mandatory**
A.11	**PHYSICAL AND ENVIRONMENTAL SECURITY**	
A.11.1	**SECURE AREAS**	
A.11.1.1	Physical security perimeter	**Mandatory**
A.11.1.2	Physical entry controls	**Critical**
A.11.1.3	Securing offices, rooms and facilities	**Non-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	**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	**Non-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	**Non-Mandatory**
A.12	**OPERATIONS SECURITY**	
A.12.1	**OPERATIONAL PROCEDURES AND RESPONSIBILITIES**	
A.12.1.1	Documented operating procedures	**Mandatory**
A.12.1.2	Change management	**Critical**
A.12.1.3	Capacity management	**Non-Mandatory**
A.12.1.4	Separation of development, testing and operational environments	**Mandatory**
A.12.2	**PROTECTION FROM MALWARE**	
A.12.2.1	Controls against malware	**Mandatory**
A.12.3	**BACKUP**	
A.12.3.1	Information backup	**Mandatory**
A.12.4	**LOGGING AND MONITORING**	
A.12.4.1	Event logging	**Critical**

A.12.4.2	Protection of log information	**Mandatory**
A.12.4.3	Administrator and operator logs	**Mandatory**
A.12.4.4	Clock synchronization	**Critical**
A.12.5	**CONTROL OF OPERATIONAL SOFTWARE**	
A.12.5.1	Installation of software on operational systems	**Critical**
A.12.6	**TECHNICAL VULNERABILITY MANAGEMENT**	
A.12.6.1	Management of technical vulnerabilities	**Critical**
A.12.6.2	Restrictions on soft-ware installation	**Mandatory**
A.12.7	**INFORMATION SYSTEMS AUDIT CONSIDERATIONS**	
A.12.7.1	Information systems audit controls	**Mandatory**
A.13	**COMMUNICATIONS SECURITY**	
A.13.1	**NETWORK SECURITY MANAGEMENT**	
A.13.1.1	Network controls	**Critical**
A.13.1.2	Security of network services	**Non-Mandatory**
A.13.1.3	Segregation in networks	**Critical**
A.13.2	**INFORMATION TRANSFER**	
A.13.2.1	Information transfer policies and procedures	**Mandatory**
A.13.2.2	Agreements on information transfer	**Mandatory**
A.13.2.3	Electronic messaging	**Mandatory**
A.13.2.4	Confidentiality or nondisclosure agreements	**Mandatory**
A.14	**SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**	
A.14.1	**SECURITY REQUIREMENTS OF INFORMATION SYSTEMS**	

A.14.1.1	Information security requirements analysis and specification	**Mandatory**
A.14.1.2	Securing application services on public networks	**Non-Mandatory**
A.14.1.3	Protecting application services transactions	**Non-Mandatory**
A.14.2	**SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES**	
A.14.2.1	Secure development policy	**Mandatory**
A.14.2.2	System change control procedures	**Non-Mandatory**
A.14.2.3	Technical review of applications after operating platform changes	**Non-Mandatory**
A.14.2.4	Restrictions on changes to software packages	**Non-Mandatory**
A.14.2.5	Secure system engineering principles	**Non-Mandatory**
A.14.2.6	Secure development environment	**Non-Mandatory**
A.14.2.7	Outsourced development	**Non-Mandatory**
A.14.2.8	System security testing	**Mandatory**
A.14.2.9	System acceptance testing	**Mandatory**
A.14.3	**TEST DATA**	
A.14.3.1	Protection of test data	**Non-Mandatory**
A.15	**SUPPLIER RELATIONSHIP**	
A.15.1	**INFORMATION SECURITY IN SUPPLIER 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	**Critical**
A.15.2	**SUPPLIER SERVICE DELIVERY MANAGEMENT**	
A.15.2.1	Monitoring and review of supplier services	**Non-Mandatory**

A.15.2.2	Managing changes to supplier services	**Non-Mandatory**
A.16	**INFORMATION SECURITY INCIDENT MANAGEMENT**	
A.16.1	**MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS**	
A.16.1.1	Responsibilities and procedures	**Mandatory**
A.16.1.2	Reporting information security events	**Mandatory**
A.16.1.3	Reporting information security weaknesses	**Mandatory**
A.16.1.4	Assessment of and decision on information security events	**Mandatory**
A.16.1.5	Response to information security incidents	**Mandatory**
A.16.1.6	Learning from information security incidents	**Mandatory**
A.16.1.7	Collection of evidence	**Non-Mandatory**
A.17	**INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**	
A.17.1	**INFORMATION SECURITY CONTINUITY**	
A.17.1.1	Planning information security continuity	**Mandatory**
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	**Non-Mandatory**

A.18.1.3	Protection of records	**Non-Mandatory**
A.18.1.4	Privacy and protection of personally identifiable information	**Non-Mandatory**
A.18.1.5	Regulation of cryptographic controls	**Non-Mandatory**
A.18.2	**INFORMATION SECURITY REVIEWS**	
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	**Critical**

Table 4.21 Critical, mandatory and non-mandatory requirements of ISM for Ethio telecom

Critical means with high importance

Mandatory means Medium importance

Non-mandatory means Low importance

4.7 Document Analysis

Regarding document analysis, Ethio telecom has some security policy and procedures which is to be carried out in the day to day activities to protect the organizational information from external and internal threat was reviewed to make sure that it is prepared according to international standard covering all the assets at the organizations premises.

Access Control Policy

This policy incorporates all current telecom infrastructure and services available throughout the company's premises. The policy takes in to account all telecom technologies and services that may be integrated in the legacy system in the future. Moreover, this policy is applicable to all governmental as well as private stakeholders, contractors and providers, customers and employees.

Data Retention and Disposal Policy

This policy applies to all electronic and hard copy records created or received in the ordinary business by Ethio telecom (which includes but not limited to email massaging, customer call detailed records (CDR's),financial data, employee documents, send/received letters, etc).

Data Center Access Policy

The Data Centre Access Policy is intended to manage, control, and access to Data Centers. This policy is required to cover all information within the organization which could include data and information that is:

- Stored on databases, computers, and transmitted across internal and public works.
- Stored on fixed media such as hard disks and disks sub-systems (A storage subsystem the supports only disk devices)

Table 4.21 Critical, mandatory and non-mandatory requirements of ISM for Ethio telecom

Even if these policies available, it has limited in content relative to the standard and also not communicated or not awareness created to the employee.

4.8 Summary

In this chapter, based on the information collected from the sampled division in Ethio telecom using questionnaires, interview, observation and document analysis, the gap towards effective information security management are identified and discussed. Hence, the result found from the information system staffs was analyzed using SPSS v.20 tool and presented in table using frequency and percentage. And in the next chapter, recommendation is given based on the result.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Overview

The final chapter presents the conclusion of the study and the recommendation based on the findings of the research. Furthermore, the chapter proposes possible ideas for future research and limitation of the Study.

5.2 Conclusion

The main objective of this research was to assess the current practice of information security management at Ethio telecom, using international standard ISO/IEC 27001 in identifying the gaps and identify the critical and mandatory requirements of ISM based on ISO/IEC270001:2013 standard for Ethio telecom.

Firstly, a literature review has been conducted to clarify terms related to information asset, information security and information security management. For this clarification; Attempts were done to examine and compare the available international standards and guidelines and ISO/IEC 27001:2013 was used in assessing the current practice in the organization. This Study was used mixed research method (questionnaire and interview) mainly to assess the current practice of information security management at Ethio telecom. Based on the gap found by the assessment the researcher identify the critical and mandatory requirements for ISM based on ISO/IEC270001:2013 standard for Ethio telecom to be adopted and deliver secured telecom services.

The finding of the study shows that Ethio telecom's physical access security management seems to be at a good position. Many people in the company are confident regarding physical security of the IT devices and systems. Access control, operations security, and business continuity aspects are also at a good position, though more improvements may be required to be considered. The company has good management of systems privilege granting and revocation. Findings of the

research show that access management records are recorded in IT service management system. This enables the company to track changes in roles of employees and security breaches.

Human resources, especially the technical staff, do not have awareness on emerging technologies. This will increase the vulnerability of the company to 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. Vendors and other equipment & systems suppliers of Ethio telecom are not assessed well for potential risks. Risks associated with asset management of the company must also be improved. According to the findings of the survey, Ethio telecom does not get its systems assessed by third parties that have the necessary tools and expertise for risk assessment. It does not also make regular risk audit by itself. This will make the company not to able to identify risks arising from business operations.

5.3 Recommendation

We can say that the successful adoption of an ISMS is important to protect information assets. It allows an organization to achieve greater assurance that its information assets are adequately protected against threats on a continual basis. It also maintains a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness. A successful ISMS can also help an organization to continually improve its control environment and effectively achieve legal and regulatory compliance. ISO standard prescribed a Plan-Do-Check-Act framework, as with other standards within the ISO umbrella. However, the revised version of this ISO 27001:2013 standard has a different approach. Without getting in to details of the standard, the organization need to adopt the following measures to successfully implement ISO 27001:2013.

Organizational Context

The first step to success really is to understand what we call a context of the organization and that simply about taking some time to understand the kind of products and services you offer to your customers and understand the kind of risks in your organization so that you can actually build your

ISMS in the right path of your business and protect those processes that actually do need to be controlled from a security point of view.

Management support

ISO 27001:2013 needs a top to bottom approach for the program to succeed. Management and Leadership are two terms in context of ISO 27001:2013 which have often been used interchangeably, which is not the case. ISO 27001 has always required a demonstration of management commitment however, the revised version ISO 27001:2013 now requires that clear leadership is demonstrated. Management is required in terms of day-to-day operation of the ISMS whereas Leadership is demonstrated by setting clear strategic goals and ensuring information security has adequate resources to its disposal. It is advisable to set up an ISO steering committee with representation from various in-scope business units. ISO 27001 isn't merely an IT function as it is commonly thought of.

Planning

ISO 27001:2013 should be treated as an independent project as the implementation of the ISMS can often be complex in nature that spreads across the breadth and width of the organization. It is essential to chart a roadmap for implementation of ISO 27001 that includes identification of tasks, roles and responsibilities, timelines and milestones.

Scoping

Organizations need to scope out the areas that ISMS will cover. This will include people, process and technology. Large organizations may choose to limit the scope of ISO 27001 implementation to a smaller subset that deals with critical business assets while leaving the rest out of scope. This not only simplifies the implementation but ensure the team is able to focus on assets that matter. All the inclusions and exclusions should be documented with justifications, especially if the organization is considering a certification against the standard.

Document the ISMS

ISMS Policy should be high level in nature, just enough for the management to define what it wants to achieve and how. The policy should have basic views of information security within the

organization, documented roles and responsibilities of all parties involved in implementation and maintenance of ISMS.

Document risk assessment methodology or framework

Risk assessment is a critical element of this program and probably the most complex element. The organization should conduct security risk assessment for all devices in scope with the help of the risk management standard ISO 31000 in order to develop their own methodology. The organization should define the methods for identification of assets (people, process, and technology), vulnerabilities, threats, impacts, likelihood and acceptable level of risk. Execute risk assessment and risk treatment. In this step organizations need to implement what has been documented in the previous step. The entire process may take a while to complete. The end goal is to be able to identify risks to all business and mission critical assets and then employ risk treatment methodology to reduce the level of risk to acceptable levels. As Zhi Xian Ng et al., (2013) stated, the absence of one vital asset from the security scoping implies that the organization has not used its resources to best advantage in addressing security risk exposure. If certain assets were not considered in the risk assessment, then they may be unprotected which lead the organization to adverse consequences such as leakage of sensitive information and interruption or destruction of critical IT services.

In addition to including all the vital assets in the scope, devices inventory need to be updated with detail description and function to identify and classify assets easily and protect from loss and unauthorized access. If the organizations want to get certified against the standard need to document a risk register which includes asset, asset values, risk values, risk treatment, inherent and residual risks and risk treatment measures or plan.

There are different methods for handling risks like:

i. Risk acceptance: Understanding and accepting risk, continuing operations or implementing controls for lowering risk where risk level can be accepted.
ii. Risk Avoidance: Avoiding risk by removing the reasons.
iii. Risk Reduction: Risk reducing is used to lower the adverse impact by executing necessary controls to an asset.

iv. Risk Sharing or Transfer: Risk transfer is used to compensate for the loss in the event of risk is happened. (i.e. insurance)

Statement of Applicability

Statement of Applicability Often called SoA, this document lists all controls from Annexure A of the ISO 27001:2013 standard with an indication of what is applicable and what isn't for the organization. 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 effectiveness of controls

In order to measure the effectiveness of implemented controls it is necessary to derive metrics or measurement criteria. Measurement criteria can be defined for a set of controls i.e. Control Objective or for individual controls. If ignored this step, results in organizations unable to measure the success of the ISMS implementation.

Implement controls

Implementation of controls could mean introducing new technologies, processes or even a change in the organizational behavior and hence this step meet with some resistance from the end user employees within the organization. How resistant the staff is depends on the nature of changes to be implemented. In order to tackle this resistance it is important to educate the end users and spread awareness as to what the organization is attempting to achieve through the implementation.

End user awareness and training

The organizations should train the staffs and educate them with regards to the dangers to the confidentiality, integrity and availability of critical assets, the risks arising out of them and hence the policies and procedures to be implemented to address those risks. As they say 'security' is incomplete without 'You!' .Which is the people within the organization. Each staff member has a role to play in helping this program succeed.

Operate and monitor the ISMS

Once implemented the ISMS needs to become an integral part of the organization's day to day activities. Organizations should monitor the ISMS using the effectiveness metrics established earlier. Documented evidence, also known as "records" should be maintained for monitoring activities. If controls are not implemented or functioning as desired organizations need to discover the reasons for this and prepare a Corrective Action Preventive Action (CAPA) plan to address this.

Internal audit

Internal audits serve to identify problems with the implementation of controls and is especially important for organizations that are planning for a certification audit. Internal audits, also referred to as "mock" audits provide the organization with an opportunity to review the implementation, documentation required to meet the organization's objectives. Any discrepancies observed need to be addressed via Corrective Action Preventive Action (CAPA) as indicated in the previous step.

Management review

Management review must be conducted at pre-determined intervals. Through these reviews the management seeks to obtain an assurance that the ISMS is operating as desired which boosts their confidence in delivering value and meeting business objectives.

5.4 Research Contribution

This study will serve as the basis for Ethio telecom to prepare, assess, and update its information security policies, procedures, and systems. Ethio telecom and other telecom companies can use the identified requirements to assess their information security management requirements associated with the inherent nature of the telecom business. Hence, Telecom companies in other developing countries having related socio-economic and cultural context can use this study to assess their information security management and practice to evaluate their stands towards international information security management standard compliance such as ISO/IEC 27001.

5.5. Limitation of the Study

The research work has got some limitations in its nature. One of the limitations is that the study was conducted using samples from only one division of Ethio telecom. This would limit information about the awareness of other employees on information security.

The other limitation of the study is that the monopoly nature of the telecom business in Ethiopia. Had there been other businesses engaged in telecom, this study would have got the chance to make a comparative study between different telecom companies. Being a single case study would also limit the amount information on the research interest.

5.6 Future Studies

Some aspects of ISM that are beyond the scope of this thesis research are recommended for future research. These are:

- Information security awareness with in the entire divisions of the organization should be done to better understand the level of information security awareness.
- This study is a single case study and specific to the telecom sector, if future research can be conducted in other different environments that would verify the findings of this study and may yield additional insights.

REFERENCES

Abdur Rahman A. (2017). Ethiopia telecoms monopoly now Africa's largest mobile operator. Retrieved December 24, 2017 from http://www.africanews.com/2017/11/16/ethiopia-telecoms-monopoly-now-africa-s-largest-mobile-operator/

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370.

Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. International Journal of Information Security Science, 2(2), 28-43.

Alan Gillies, (2011) "Improving the quality of information security management systems with ISO27000", The TQM Journal, Vol. 23 Issue: 4, pp.367-376.

Al-Kalbani, A. (2017). A compliance based framework for information security in e-government in Oman.

Anderson, J.M. (2003). Why we need a new definition of information security, Computers & Security, 22(4): 308-313.

Anene, L. N., & Annette, L. S. (2007). An Architectural and Process Model Approach to Information Security Management. Lawrence Technological University.

Ardian Berisha, (2016). Applying ISO/IEC 27001 in the Telecommunications Industry. Retrieved from https://pecb.com/article/applying-isoiec-27001-in-the-telecommunications-industry. Accessed Date: 12 June 2018.

Ashenden, D. (2008). Information security management: a human challenge, Information Security Technical Report, 13(4): 195-201.

Aydoğmuş, E., 2010. Assessment of Information Security Maturity Levels and ISO/IEC 27001:2005 Compliance of Organizations in Turkey, Istanbul: İ.T.Ü.

Barlette, Y., & Fomin, V. V. (2010). The adoption of information security management standards. Information resources management: concepts. Methodologies, tools and applications. IGI Global, Pennsylvania, 69-90.

Beebe, N. L., & Rao, V. S. (2009). Examination of organizational information security strategy: A pilot study. AMCIS 2009 Proceedings, 417.

Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. *British Journal of Management*, 18(1), 6377.

Bishop, M. (2003). Computer Security: Art and Science. Boston, MA, USA: Addison-Wesley.

Brenner, J. (2007). ISO 27001: Risk management and compliance. Risk management, 54(1), 24.

BSI-Standard 100-1 (2008). Information Security Management Systems (ISMS), Retrieved February 17, 2018 from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

C.R.Kothari (2007).Research methodology: Methods &Techniques. 2nd ed. India: New Age International (P) Ltd., Publishers.

Caralli, R. (2004). The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management. Carnegie-Mellon Engineering Institute Journal Article. Retrieved April 9, 2018 from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14393.pdf

Caralli, R. A., & Wilson, W. R. (2004). The challenges of security management. Pittsburgh, PA: CERT, Software Engineering Institute, Carnegie Mellon University.

Cazemier, J.A., Overbeek, P.L. and Peters, L. M. (2000) Security Management. IT Infrastructure Library Series (Part 14). UK: Stationery Office.

CESG (2015). Security_Procedures_Telecommunication_Systems_and_Services. Retrieved April 3, 2018, from https://www.ncsc.gov.uk/content/files/Security_Procedures_Telecommunication_Systems_and_Services__-_issue_3.0_Dec_2015.pdf

Cheol-Soon Park, Sang-Soo Jang, Yong-Tae Park (2010). A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance, IJCSNS International Journal of Computer Science and Network Security, VOL.10, pp.10-21.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. 2007. "Management of Information Security: Challenges and Research Directions," Communications of the Association for Information Systems (20), pp 958- 971.

Collis, J., & Hussey, R. (2009). Business Research: A Practical Guide for Undergraduate and Postgraduate Students. London: Palgrave Macmillan.

Creswell, J. W., Klassen, A. C., Plano Clark, V. L., & Smith, K. C. (2011). Best practices for mixed methods research in the health sciences. Bethesda (Maryland): National Institutes of Health (2013):541-545

Daniel, G. (2017). Assessment of the effectiveness of card banking security in the Ethiopian financial sector. Addis Ababa: Unpublished Master's Thesis.

Danielito V. (2012). Information Security Governance – Telecommunication Industry, Retrieved February 17, 2018 from https://dcvizcayno.wordpress.com/2012/04/11/information-security-governance-telecommunication-industry/

Dean, C. V., Achilles, A. A., & Hubert, S. F. (2008). Integrating Qualitative and Quantitative Methods for Organizational Diagnosis. Possible Priming Effects? Auburn University, Alabama. Journal of Mixed Methods Research, Volume 2 number1, Sage Publications.

Department for Business, I. S. (2013). UK cyber security standards: research report. Retrieved April 9, 2018 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

Dinesh S. (2015). How Important Is ISO 27001 Compliance (ISMS Implementation) to an Organization. Retrieved April 15, 2018 from https://securitycommunity.tcs.com/infosecsoapbox/articles/2015/03/03/how-important-iso-27001-compliance-isms-implementation-organization

ENISA (2012). Shortlisting network and information security standards and good practices

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361.

Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.

Farn, K. J., Lin, S. K., & Fung, A. R. W. (2004). A study on information security management system evaluation—assets, threat and vulnerability. Computer Standards & Interfaces, 26(6), 501-513.

Finne, T. (2000). Information systems risk management: key concepts and business processes, Computers & Security, 19(3): 234-242.

Gordon, L.A. and Loeb, M.P. (2002).The economics of information security investment, ACM Transactions on Information and System Security, 5(4): 438-457.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). Security management standards: a mapping. Procedia Computer Science, 100, 755-761.

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.

Hou, Y. (2014). Understanding Organizational Response to Institutional Pressures in Information Security Management: Two Chinese Case Studies (Doctoral dissertation, University of Manchester).

Hu, Q., Hart, P. and Cooke, D. (2007). The role of external and internal influences on information system security - a neo-institutional perspective, Journal of Strategic Information System, 16(2): 153-172.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information security technical report, 13(4), 247-255.

International Organization for Standardization(ISO) (2012), Information technology - Security techniques - Governance of information security - Requirements, ISO/IEC FDIS 27014, ISO & IEC, Published in Switzerland.

ISACA (1996). Control Objectives for Information and related Technology (COBIT). Retrieved from: http://www.the281group.com/index.php/control-objectives-for-information-and-related-technology-cobit. Accessed Date: 26 May 2018.

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

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.

ISO/IEC FDIS 27001, (2005). Information technology Security techniques Information security management systems Requirements, pp.1-34.

Jimmy (2012). COBIT in Relation to Other International Standards. Retrieved from: http://www. COBIT-in-Relation-to-Other-International-Standards.aspx.htm. accessed date: 18 Feb, 2018.

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. Communications of the ACM, 52(1), 126-129.

Joobin Choobineh, Gurpreet Dhillon, Michael R. Grimaila, Jackie Rees (2007). Management of Information Security: Challenges and Research Directions, Communications of the Association for Information Systems Volume 20, pp.958-971.

Karamanlis, M., & Καραμανλής, Μ. (2016). Information Security Management System toolkit (Master's thesis, Πανεπιστήμιο Πειραιώς).

Kosutic, D., 2014. ISO27001 Standard. [Çevrimiçi] Available at: http://blog.iso27001standard.com/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/ [Erişildi: April 2018].

Kotrlik, J. W. K. J. W., & Higgins, C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal,* 19(1), 43.

Krutz, R. & Vines, R. (2001). CISSP Prep Guide: Mastering the Ten Domains of Information Security. New York, N.Y.: Wiley & Sons.

Kumar, R. L., Park, S., and Subramaniam, C. (2008). Understanding the value of countermeasures portfolios in information systems security. Journal on Management Information Systems, 25, 241-279.

Lane, T. (2007). Information security management in Australian Universities: An exploratory analysis (Doctoral dissertation, Queensland University of Technology).

Lisa M. Given (2008). The SAGE Encyclopedia of Qualitative Research Methods. SAGE Publications, 1 & 2.

Ma, Q., Schmidth, M.B. and Pearson, J.M. (2009), "An integrated framework of information security management", Review of Business, Vol. 30 No. 1, pp. 58-69.

Mario Spremic (2011). Standards and Frameworks for Information System Security Auditing and Assurance, Proceedings of the World Congress on Engineering Vol I London, U.K.pp.978-988.

Mete Emina_gao_glu, Erdem Uc, Sxaban Eren (2009). The positive outcomes of information security awareness training in companies A case study, information security technical report, pp.223-229.

Mohammed, A., & Karen, N. (2009). Proceedings of the 7th Australian Information Security Management Conference: A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.

Myers, M. D. (2009). Qualitative Research in Business and Management. London: Sage Publications.

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

Neuman, W. L. (2003). Social Research Methods: Qualitative and Quantitative Approaches. London: Pearson Education.

Oliveira Alves, G.A.; Costa Carmo, L.F.R.; Almeida, A.C.R.D., (2006) Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG), Business-Driven IT Management, BDIM '06, pp.71,80. [Online]. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1649213&isnumber=34578 (Accessed 29 April 2018)

Patton, M. (2002). Qualitative Research and Evaluation Methods. London: Sage Publications.

Peltier, T. R. (2010). Information security risk analysis. Auerbach publications.

QAI Global Services (2014). Telecom--QAI Global. Retrieved October 14, 2017 from https://www.qaiglobalservices.com/CMMI-Six-Sigma-Consulting-Telecom-Sector.html

Rezakhani, A., Hajebi, A., & Mohammadi, N. (2011). Standardization of all information security management systems. International journal of computer Application, 18(8).

Sarantakos, S. (2005). Social Research. New York: Palgrave Macmillan.

Schneier, B. (2004) Secrets & Lies: Digital Security in a Networked World. Indianapolis, Ind.: Wiley Publishing Inc.

Sebastian V. (2016). Applying ISO/IEC 27001 in the Telecommunications Industry. Retrieved February 17, 2018 from https://www.linkedin.com/pulse/applying-isoiec-27001-telecommunications-industry-sebastian-vogels

Susanto, H., & Almunawar, M. N. (2015). Managing Compliance with an Information Security Management Standard. In Encyclopedia of Information Science and Technology, Third Edition (pp. 1452-1463). IGI Global.

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. International Journal of Critical Infrastructure Protection, 2(3), 95-109.

Teece, D.J. (2010). Business models, business strategy and innovation. Long range planning, 43(2), 172-194.

Von Solms, B. and von Solms, R. (2004), "The 10 deadly sins of information security management", Computers & Security, Vol. 23 No. 5, pp. 371-376.

Von Solms, E. & Von Solms, S.H. (2000) Information Security Management through Measurement. In S. Qing & J.H.P. Eloff (Eds.) Information Security for Global Information Infrastructures (pp. 59 – 68). Norwell, MA: Kurwell Academic

Whitman, M. & Matthord, H. J., 2011. Principles of Information Security. Boston: Course Technology.

Whitman, M., & Mattord, (2004) Management of Information Security. Boston, Ma: Thomson.

Yeniman Yildirim, E., Akalp, G., Aytac, S., and Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprise: a case study from turkey. International journal of information management, 31(4), 360-365.

Yigezu, B. J. (2011). Information System Security Audit Readiness. Case study: Ethiopian Government Organizations.

Yin, R. K. (2009). Case Study Research: Design and Methods. London: Sage Publications.

Zafar, H. and Clark, J. G. (2009). Current state of information security research in IS, Communications of the Association for Information Systems, 24(1): 557-596.

Zaidah Zainal (2007). Case study as a research method. Journal Kemanusiaan

Zhi Xian Ng, Atif Ahmad, Sean B. Maynard (2013). Information Security Management: Factors that Influence Security Investments in SMES, Australian Information Security Management Conference, Edith Cowan University, pp.60-73.

APPENDICES

Appendix A: Survey Questionnaire

Dear Participant,

My name is Yemane Gebrehiwot, a postgraduate student at Addis Ababa University, School of Information Science. As partial fulfillment of my MSc degree program in Information Science, I am conducting a research work lies on assessing information security management using an ISO 27001:2013 framework: a case study at Ethio telecom. Hence, I am kindly inviting you to participate in this research by completing the attached survey questions. I thank you in advance, with great appreciation, that you spend a few minutes of your valuable time to answer all the questions in the questionnaire.

This survey is anonymous. No one, including the researcher, will associate your responses with your identity. Your participation is voluntary. You may choose not to take the survey, to stop responding at any time, or to skip any question that you do not want to answer. Your response is extremely important and valuable for the success of the research to achieve the objective of the study by indicating possible gaps, if any, and possible solutions that need to be taken by concerned parties.

If you choose to participate in this research, please answer all questions as honestly as possible and return the completed questionnaires promptly. If you want any additional clarification or further information or have questions, please don't hesitate to contact me with either of the contact addresses below.

Mobile Number: +251- 911-502406

Email: yemanegb@gmail.com

Thank you for your willingness and valuable time.

Sincerely,

Term definitions

ISO/IEC 27001:2013 (ISO 27001) is the international standard that describes best practice for an ISMS (information security management system).

Information security management system (ISMS): is a defined, documented management system that consists of a set of policies, processes, and systems to manage risks to organizational data, with the objective of ensuring acceptable levels of information security risk.

A data center: is a facility that centralizes an organization's IT operations and equipment, as well as where it stores, manages, and disseminates its data. Data centers house a network's most critical systems and are vital to the continuity of daily operations.

Security patch management: security patch management process has become a critical component in the maintenance of security on any information system. As more and more software vulnerabilities are discovered and therefore need updates and patches, it is essential that system administrators manage the patching process in a systematic and controlled way. Information security responsibilities

De-Militarized Zone (DMZ) is a special local network configuration designed to improve security by segregating computers on each side of a firewall. It is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet.

A **business continuity plan (BCP**) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions.

Your answer has the following meaning:

- **Yes =** the organization is doing it fully
- **No =** the organization is not doing it fully
- **Partial =** incomplete and not fully exercised in the organization
- **I don't know =** does not have the information in the organization

Instruction: This questionnaire has four sections. Please put a "□ "sign in the square bracket [ ] for each item. You can also write your opinion or justification for open ended question

Part I: Respondent Information

Job Title: ……..

Sex: [ ] Male [ ] Female

Education: [ ] Diploma [ ] Degree [ ] Masters [ ] PHD

Work Experience: [ ] 1-5years [ ] 6-10 years [ ] 11-15years [ ] above 15 years

Part II Administrative, Security Policy and Standards

1. Does the organization have security policy document, approved by management to ensure the security of your organization's information system? (ISP)
   [ ] Yes [ ] Partial [ ] No [ ] I don't know
2. If your answer is yes for question #1, are policies properly communicated to employees? (ISP) [ ] Yes [ ] Partial [ ] No [ ] I don't know
3. Are information security policies reviewed and updated periodically? (ISP)
   [ ] Yes [ ] Partial [ ] No [ ] I don't know
4. Are reviews conducted when circumstances change? (ISP)
   [ ] Yes [ ] Partial [ ] No [ ] I don't know
5. If the organization has information security policy, did stakeholders, such as Security specialists, technical staff, HR administrators, legal advisors, internal auditors, risk and compliance staff, and top management involve in the policy development? (SADM)
   [ ] Yes [ ] Partial [ ] No [ ] I don't know
6. Does the information security policy consider all stakeholders such as employees, contractors, suppliers/venders, regulatory and customers who have access to Ethio telecom's network? (SADM)
   [ ] Yes [ ] Partial [ ] No [ ] I don't know

7. Are contacts with relevant authorities (law enforcement etc.) and special interest groups defined? (OIS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
8. Does Ethio telecom use industry standards or frameworks in the process of implementation of its information systems security?
   [ ] Yes [ ] Partial [ ] No [ ] I don't know
9. Does the organization conduct formal risk management activity before developing an information security policy? (OIS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
10. Are risks from third party access identified and appropriate security controls implemented?
    [ ] Yes [ ] Partial [ ] No [ ] I don't know (SR)
11. Do you think that lack of experienced staff on international standards, lack of local information security management framework/standard, and budget are problems or challenges that hinder the implementation of information security management system in the organization? (OIS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
12. Are roles, responsibilities, and authorities for information security assigned and communicated? (ISP) [ ] Yes [ ] Partial [ ] No [ ] I don't know
13. Does Ethio telecom have a dedicated individual (or individuals) with responsibility for information security? (HRS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
14. Does the management support in information security assurance process? (OIS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
15. Does Ethio telecom have annual budget for staff information security awareness program and security technical training? (CS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
16. Do you think that separating information security team from other IT functions is advantageous from security assurance perspective? (OIS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
17. Are duties and areas of responsibility separated in order to reduce opportunities for unauthorized modification or misuse of information or services? (OIS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
18. Do all projects go through some form of information security assessment? (OIS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know

19. Are rules for secure handling of mobile devices (like Smartphone, laptop & others) defined? (OIS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
20. Does the organization audit its information systems security in a regular basis? (CO)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
21. Does the organization outsource IT systems security audit to third party? (CO)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
22. Does the company have defined information asset inventory, classification scheme or guidelines in place; which will assist in determining how information is to be handled and protected? (AM) [ ] Yes [ ] Partial [ ] No [ ] I don't know
23. Does all information assets have a clearly defined owner who is aware of their responsibilities? (AM) [ ] Yes [ ] Partial [ ] No [ ] I don't know
24. Is there a formal procedure governing on how removable media that contain sensitive information is transported and disposed? (AM)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
25. Does employees' written job description include responsibility for information security? (HRS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
26. Does Ethio telecom invite employees to be involved in the development of information security policies in order to encourage a sense of ownership? (SADM)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
27. Are employees and contractors sign confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment? (HRS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
28. Do supplier agreements include requirements to address information security within the service and product supply chain? (SR)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
29. Does all employees of Ethio telecom and third party users receive appropriate information security awareness and regular updates on Ethio telecom's policies and procedures? (CS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
30. Does the technical staff have awareness about emerging technologies and related control issues? [ ] Yes [ ] Partial [ ] No [ ] I don't know

31. Does Ethio telecom have written incident management and formal reporting procedure to handle security incidents? (ISIM) [ ] Yes [ ] Partial [ ] No [ ] I don't know
32. Does Ethio telecom have an approved business continuity plan? (ISBCM)
[ ] Yes [ ] Partial [ ] No [ ] I don't know
33. Does Ethio telecom have disaster recovery plan for its business critical services which is exercised and tested? (ISBCM) [ ] Yes [ ] Partial [ ] No [ ] I don't know
34. Does Ethio telecom perform periodical penetration testing of their infrastructure? (SADM)
[ ] Yes [ ] Partial [ ] No [ ] I don't know

Part III. Physical and Environmental Security

Physical security is critical to achieving confidentiality and availability goals of mission critical facilities like server rooms/ data center.

35. What kind of security enforcement is/are used to protect IT critical facilities? (PES)
    a) Alternate power source like generator [ ] Yes [ ] Partial [ ] No [ ] I don't know
    b) air conditioning [ ] Yes [ ] Partial [ ] No [ ] I don't know
    c) water leakage management and Fire extinguisher systems
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
    d) Fences and /or Human security guards [ ] Yes [ ] Partial [ ] No [ ] I don't know
    e) Door Access system (Biometrics / card/ PIN), conventional key and CCTV camera
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
36. Are perimeter security controls defined and used to protect areas that contain sensitive or critical information. (PES) [ ] Yes [ ] Partial [ ] No [ ] I don't know
37. Are visitors and contractors supervised when they are visiting your server rooms? (PES)
[ ] Yes [ ] Partial [ ] No [ ] I don't know
38. Does authorization and checking occur on equipment entering or leaving your site? (PES)
[ ] Yes [ ] Partially [ ] No [ ] I don't know

Part IV. Technical and Operational Security

39. Does the organization have security patch management procedure to know vulnerabilities? (OS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
40. Are system logs monitored and logged? (OS) [ ] Yes [ ] Partial [ ] No [ ] I don't know

41. When a new system or device (such as Firewalls, Routers, Switches etc.) is installed on the network what kind of steps are taken? (AC)
    a) Default usernames and passwords will be changed immediately. (AC)
       [ ] Yes [ ] Partial [ ] No [ ] I don't know
    b) Access to system resources will be restricted to only the individuals that are authorized to use those resources. (AC) [ ] Yes [ ] Partial [ ] No [ ] I don't know
    c) Any unnecessary protocol, services and ports will be disabled /closed. (AC)
       [ ] Yes [ ] Partial [ ] No [ ] I don't know
42. Is there a controlled change management process in place? (OS)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
43. Is there network management process in place to manage and control information in the system? (CS) [ ] Yes [ ] Partial [ ] No [ ] I don't know
44. Is there a formally defined user access control policy document for granting access to multi-user information systems and services? (AC) [ ] Yes [ ] Partial [ ] No [ ] I don't know
45. Are access rights updated when there is a change in the user situation (e.g.: department/section change or termination)? (AC)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
46. Does the organization have any procedures and processes to review user (user registration and de-registration)? (AC) [ ] Yes [ ] Partial [ ] No [ ] I don't know
47. Does the organization have password guidelines (about its complexity, change period, password reset, access attempt and lockout ...etc.) for the users in selecting and maintaining of password? (AC) [ ] Yes [ ] Partial [ ] No [ ] I don't know
48. Is there an internal firewall which is between intranet and DMZ (demilitarized zone)? (AC)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
49. Is there an external firewall which is between the DMZ (demilitarized zone) and internet or outside world? (AC) [ ] Yes [ ] Partial [ ] No [ ] I don't know
50. If the answer under #48 & # 49 is Yes, have you used different vendors firewall for the internal and external perimeter firewall? (AC)
    [ ] Yes [ ] Partial [ ] No [ ] I don't know
51. Does the organization implement internetwork management system like Cisco works, Cisco Access Control server or Cisco Security Management Systems? (AC)

[ ] Yes [ ] partially [ ] No [ ] I don't know

52. Does the organization implement wireless network in its compound? (OIS)

[ ] Yes [ ] partial [ ] No [ ] I don't know

53. If the answer of # 52 is Yes, Have you used authentication and encryption technologies like WEP or WPA or any other for Wireless LAN network security? (OIS)

[ ] Yes [ ] partial [ ] No [ ] I don't know

54. Is an antivirus installed and regularly updated on the computers that exist in the organization? (OS) [ ] Yes [ ] partial [ ] No [ ] I don't know

55. Does all the traffic originating from untrusted network in to the organization flittered by firewall and web security to protect malicious attacks? (OS)

[ ] Yes [ ] Partial [ ] No [ ] I don't know

56. Do you have any documented operating procedures such as backup procedure, equipment maintenance procedure, etc.? (OS)

[ ] Yes [ ] Partial [ ] No [ ] I don't know

57. Is backup of business critical information taken regularly? (OS)

[ ] Yes [ ] Partial [ ] No [ ] I don't know

58. Are Internet line and data line for business critical services separated? (OS)

[ ] Yes [ ] Partial [ ] No [ ] I don't know

59. Are clocks on all IT systems synchronized? (OS) [ ] Yes [ ] Partial [ ] No [ ] I don't know

60. Does the organization have any authentication mechanism for challenging external connections? (C) [ ] Yes [ ] Partial [ ] No [ ] I don't know

If your answer to question # 60 is yes, which of the following mechanisms are used?

a) Cryptography based technique (Encryption & Digital signature) (C)

[ ] Yes [ ] Partial [ ] No [ ] I don't know

b) hardware or software tokens (C) [ ] Yes [ ] Partial [ ] No [ ] I don't know

61. Is there a culture of conducting security requirement study before systems development and test its security related issue in the organization? (SADM)

[ ] Yes [ ] Partial [ ] No [ ] I don't know

END. THANK YOU!

Appendix B: Interview Guide

1) Information about you: Your job position now?

2) If you have developed ISMS in your organization, what kind of standard or framework the organization employed in the process of ISMS development? If not developed ISMS, what are the reasons?

3) If you developed ISMS in your company, what is/are the drawback(s) and strength of the standard that you have employed in ISMS development?

4) What issues concern you most about the information security in Ethio telecom? Please support your answers with justification?

5) How the organization identifies its security requirements prior to selecting best practices or controls?

6) What Requirements do you think are critical to the success of Ethio telecom's information security management? Please support your answers with justification?

7) From what aspects do you think Ethio telecom's information security management can be improved?

8) What is your opinion about the pros and cons of separating Information security management team from other IT staffs structurally in IT department?

Appendix C: ISO/IEC 27000-series information security standards

Standard	Published	Title	Notes
ISO/IEC 27000	2014	Information security management systems - Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary; FREE!
ISO/IEC 27001	2013	Information security management systems requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls

ISO/IEC 27003	2010	Information security management system implementation guidance	Basic advice on implementing ISO27k
ISO/IEC 27004	2009	Information security management Measurement	Basic (and frankly rather poor) advice on information security metrics
ISO/IEC 27005	2011	Information security risk management	Discusses risk management principles; does not specify particular methods for risk analysis etc.
ISO/IEC 27006	2011	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies
ISO/IEC 27007	2011	Guidelines for information security management systems auditing	Auditing the management system elements of the ISMS
ISO/IEC TR 27008	2011	Guidelines for auditors on information security management systems controls	Auditing the information security elements of the ISMS
ISO/IEC 27009	DRAFT	Application of ISO/IEC 27001 - requirements	Sector- or service-specific certifications (possibly)
ISO/IEC 27010	2012	Information security management for inter-sector and inter-organizational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure"
ISO/IEC 27011	2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051"
ISO/IEC 27013	2012	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"
ISO/IEC 27015	2012	Information security management guidelines for financial services	Applying ISO27k in the finance industry

ISO/IEC TR 27016	2014	Information security management – Organizational economics	Economics applied to information security
ISO/IEC 27017	DRAFT	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
ISO/IEC 27018	DRAFT	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing
ISO/IEC TR 27019	2013	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!)
ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (i.e. resilience, incident management and disaster recovery) for ICT, supporting general business continuity
ISO/IEC 27032	2012	Guidelines for cybersecurity	Despite the curious title, it is actually about Internet security
ISO/IEC 27033	-1 2009	Network security overview and concepts	Various aspects of network security; gradually updating and replacing ISO/IEC 18028
	-2 2012	Guidelines for the design and implementation of network security	
	-3 2010	Reference networking scenarios threats, design techniques and control issues	
	-4 2014	Securing communications between networks using security gateways	
	-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	

	-6 DRAFT	Securing IP network access using wireless	
ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard
	-2 DRAFT	Organization normative framework	
	-3 DRAFT	Application security management process	
	-4 DRAFT	Application security validation	
	-5 DRAFT	Protocols and application security control data structure	
	-6 DRAFT	Security guidance for specific applications	
	-7 DRAFT	Application security control attribute predictability	
	-8 DRAFT	Protocols and application security controls data structure – XML schemas	
ISO/IEC 27035	2011	Information security incident management	Replaced ISO TR 18044; now being split into three parts
ISO/IEC 27036	-1 DRAFT	Information security for supplier relationships – Overview and concepts	Information security aspects of ICT outsourcing and services
	-2 DRAFT	Information security for supplier relationships – Common requirements	
	-3 2013	Information security for supplier relationships – Guidelines for ICT supply chain security	
	-4 DRAFT	Information security for supplier relationships –	

ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	First of several IT forensics standards
ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents
ISO/IEC 27039	DRAFT	Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)	IDS/IPS
ISO/IEC 27040	DRAFT	Storage security	IT security for stored data
ISO/IEC 27041	DRAFT	Guidelines for assurance for digital evidence investigation methods	Assurance is critically important for all forms of forensics: the courts demand it
ISO/IEC 27042	DRAFT	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
ISO/IEC 27043	DRAFT	Digital evidence investigation principles and processes	The basic principles of IT forensics investigations
ISO/IEC 27044	DRAFT	Guidelines for security information and event management (SIEM)	SIEM
ISO 27799	2008	Health informatics - Information security management in health using ISO/IEC 27002	Developed by a different committee; tailored advice for the healthcare industry

ISO/IEC 27000-series information security standards; adapted from Karamanlis, (2016).

Appendix D: Annex A – Reference controls, control objectives and clause

Section	Name of Controls	Control Objectives	Number of Clauses
A.5	Information security policies.	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	2
A.6	Organization of Information Security	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	7
A.7	Human Resource Security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	6
A.8	Asset Management	To identify organizational assets and define appropriate protection responsibilities.	10
A.9	Access Control	The controls in this section aim to limit access to information and information assets considering business needs, by means of formal processes to grant or revoke access rights. The controls consider either physical or logical access, as well as access made by people and by information systems.	14
A.10	Cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information	2
A.11	Physical and Environmental Security	The controls in this section aim to prevent unauthorized access to physical areas, as well as to protect equipment and facilities that if compromised, by human or natural intervention, could affect information assets or business operations.	15
		The controls in this section aim to ensure that the operation of information processing facilities, including operating systems, are secure and protected against malware and data loss.	

A.12	Operational Security	Additionally, controls in this section require the means to record events and generate evidence, periodic verification of vulnerabilities, and the establishment of precautions to prevent audit activities from affecting operations.	14
A.13	Communications Security	The controls in this section aim to protect the network infrastructure and services, as well as the information that travels on them.	7
A.14	System Acquisition, Development and Maintenance	The controls in this section aim to ensure that information security is considered in the system development life cycle.	13
A.15	Supplier Relationships	The controls in this section aim to ensure that outsourced activities performed by suppliers also consider information security controls, and that they are properly managed by the organization.	5
A.16	Information Security Incident Management	The controls in this section aim to provide a framework to ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner and consider the preservation of evidence as required, as well as the improvement of processes to avoid recurrence.	7
A.17	Information Security aspects of Business Continuity Management	The controls in this section aim to ensure the continuity of information security management during adverse situations, as well as the availability of information systems.	4
A.18	Compliance	The controls in this section aim to provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and to ensure independent confirmation that information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.	8