ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF INFORMATION SECURITY MATURITY LEVEL ON ETHIOPIAN PUBLIC UNIVERSITIES

By:

NEBYU EJERSSA

JUNE, 2018

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF INFORMATION SECURITY MATURITY LEVEL ON ETHIOPIAN PUBLIC UNIVERSITIES

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: Nebyu Ejerssa

Advisor: Getachew Hailemariam (PhD)

June, 2018

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF INFORMATION SECURITY MATURITY LEVEL ON ETHIOPIAN PUBLIC UNIVERSITIES

By: Nebyu Ejerssa

Name and signature of Members of the Examining Board

Getachew Hailemariam (PhD)	----------	----------
Advisor	Signature	Date
Gashaw kebede (PhD)	----------	----------
Examiner	Signature	Date
Lemma Lessa (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: _____

Nebyu Ejerssa

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

Advisor's Signature: _____

Getachew Hailemariam (PhD)

ACKNOWLEDGEMENTS

Foremost, thanks to God, the Almighty, for his blessings throughout my research work to complete the research successfully.

In this wonderful opportunity, it is a pleasure to thank the people who helped me during the whole process of the thesis.

Firstly, I would like to express my sincere gratitude to my research Advisor, Dr. Getachew Hailemariam for his strong support in research process. I had a great fortune to study under his supervision, and I am very grateful for his guidance and encouragement.

Then, I would like to thank all of my family members and my friends for their caring, sacrifices, encouragements and being there for me throughout the study.

Finally, I would like sincerely to express my gratitude to all individuals who have been showing me their willingness when I needed their help during the whole process of the thesis.

ABSTRACT

Information security has become one of the most important and challenging issues facing today's organizations including universities. This study attempts to assess the current maturity level of information security management practice in Ethiopian public universities. It investigates the current maturity level of information security implementation in Ethiopian public universities and analyze the gap to give recommendations for future improvements.

The study used Qualitative and Quantitative methods (A mixed method) to meet the research objectives set out. Data was collected from the selected 10 sample universities through Questionnaire and interview as primary data source besides to the analysis of written documents which is used as a secondary data Sources.

This research answers the following research questions: What is the current maturity level of information security implementation in Ethiopian public universities sector? What are the uppermost and lowermost maturity scored information security controls in Ethiopian public universities? How could potential improvements in information security be achieved in Ethiopian public universities?

The study findings indicate that the information security control environment in public universities is insufficient. From the analysis conducted which is based on the SSE-CMM maturity model assessment criteria range from level 0 (none) to level 5 (optimistic), the results showed that the maturity level of information security in Ethiopian public universities is 2.16, which means the level of security is at level 2 (repeatable but intuitive). This referee to the institutions have a pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency.

The research helps to improve the current understanding of information security issues and supports the applicability of information security management as a strategically important function for Ethiopian public universities. Also, universities can utilize the research result to structure their information security management system.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

CIA - Confidentiality, integrity and availability

IEC - International Electro Technical Commission

IT – Information Technology

ICT-Information and communications technology

IS - Information Systems

ISP - Information Security Policy

ISM – Information security management

ISMS – Information security management system

ISO International Standardization of Organization

SSE-CMM - System Security Engineering Capability Maturity Model

CHAPTER ONE: INTRODUCTION

The purpose of this chapter is to set the background of the study. It begins with a brief overview of the issues on the important of information asset and its security in organizations including higher education institutions. The second section deals with the research problem subsequently by the basic research questions are presented. This is followed by presentation of the objectives of the study. Then the rationale significant contribution and the scope of the study is explained in the fifth and sixth sections respectively. Finally, the organization of the thesis is presented.

1.1. Background

Organizations have different assets; one of those assets is information. This most valuable asset in the organization is considered as a critical resource, enabling the organization to achieve its goals. The ultimate goal of information security is to protect the interest of those who depend on information technology and communication systems that contains information from harm (Mehdi , Hamid , & Hashem , 2012).

Information is a collection of data that have meaning in a particular context and used to transfer the concept that has value in certain circumstances (Fulford & Doherty , 2003). Information security protects information systems against unauthorized access or manipulation of information, whether in storage, processing or exchange and the exclusion of services for authorized users or providing services to unauthorized users that includes these necessary actions to discover, document and dealing with such threats (Mehdi , Hamid , & Hashem , 2012)

Information security has become one of the most important and challenging issues facing today's organizations. Information security is defined as the activity to protect information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities (Ladan, Yari, & Khodabandeh, 2006). This makes Information security to be one of the critical issues facing any organization worldwide including higher learning institutes. Information security includes technical measures and management measures. Valuable assets understandably require appropriate protection. This is

underpinned by recognition of information as valuable asset and strategic resource. Having appropriate and effective information security control mechanisms in place to ensure the availability, confidentiality and integrity of information is therefore critical to the process of security management (Mehdi , Hamid , & Hashem , 2012).

Information Security Management mainly concern with the strategic, tactical and operational issues that surround the planning, analysis, design, implementation and maintenance of organization's information security programs. There are numerous standards, frameworks, models and supporting tools available for information security management. Some of them are general-purpose and, others address specifically. The Standards and good practice frameworks can only provide generic guidance and each organization must find its own way to put this knowledge into real-world practice (Noli , 2016).

According to Tim (2007), Higher Learning Institutions now a day rely on information technology for conducting the daily works including, administration, teaching, learning and research. Applying information security to universities IT systems is very important to maintain overall business continuity. The process of well implementing information security management in the Higher Learning Institutions sector is challenging because university environment involves different academic student needs and compliance mandates. This leads to a divergent demand on securing the IT infrastructure. Likewise, Universities in Ethiopia are progressively using information technology (IT) for essential business operations including administration, teaching, learning and research.

1.2. Problem Statement

Information security management refers to the controls that an organization needs to implement to ensure the safety of its information asset. Information security management is a series of management activities with the aim of protecting and securing information assets within the framework of the organization in which information system is running (Solms, 1998). Information security management has become an important business responsibility and accountability escalated up to the higher level of management in organizations (Noli , 2016).

Organizations need a systematic information security approach that is used for the arrangement or structuring of information security components to implement information security in an effective manner to mitigate risks in an organization (Qingxiong & Pauline , 2008).

The challenge of IT governance and security management is no exception. Like other organization, Universities are increasingly admitting the importance of information security to protect business and confidential information. Universities have adopted information systems and the related technologies so as to gain a competitive edge. There is a dependence on activities associated with creating, using and sharing information for universities core teaching, learning and research functions (Tim , 2007).

Higher Learning Institutions are directly impacted by their reliance on and use of information technology resources. In this era effective control of operations and strong strategies are associated with management of quality information. The aspect of readily available information means that universities are affected by their dependence on information and technology resources, systems and the underlying structures that form the basis for this technologies and systems (Bichanga & Obara , 2014).

When an information system in an organization, including higher education institution, is neither safe nor well-protected, then there will be a risk. Lack of control and prevention of data lost that caused by disaster or incident as well as inadequate recovery after the disaster will harm the institutions to continue its business. Information security could not only be based on the tools of information security technology, but also should be backed up by a good understanding of the people in the university about what thing must be protected and how to provide a right solution (Puspita , Nadiailhaq , & Candiwan , 2013).

According to a study by Bichanga and Obara (2014), on challenges facing information systems security management in Eastern Africa, shows that higher learning institutions are facing security vulnerabilities. It is stated that, In the Past four years Universities have been experienced many cases of security breaches. Some of the security issues were; students hacking into information systems and altering their grades, unprecedented challenge of hacking the

institutional mailing system, unauthorized use of systems at work by employees with vested interests, Non-work-related upload/download, transmission of confidential data, and unauthorized use of internet.

Likewise, one of the greatest challenges facing universities in Ethiopia today is how to effectively manage the security of information systems that support teaching, learning and research activities. Recently, information security issues and incidents have been witnessed in public and private universities in Ethiopia. Several studies have been carried out in the area of information security in other sectors like banking sector but the educational sector has been left behind. There is lack of structured approach or framework for the effective management of information security in the higher learning institutions in Ethiopia. (Source: researcher's experience and communication with IT experts in education sector).

Therefore, due to the above facts Information Security management must be well considered to provide higher learning institutes with guidelines on how to address the integrity, availability, and confidentiality of information resources by first assessing their current practice in securing their information and information systems. Thus, the study aim is to assess the current maturity level of information security implementation in Ethiopian public universities and analyze the maturity result to give recommendations for future improvements.

1.3. Research Questions

The research process explores and answers the following research questions.

i. What is the current maturity level of information security implementation in Ethiopian public universities sector?
ii. What are the uppermost and lowermost maturity scored information security controls in Ethiopian public universities?
iii. How could potential improvements in information security be achieved in Ethiopian public universities?

1.4. Research Objectives

1.4.1. General Objective

The general objective of this research is to assess the current maturity level of information security implementation in Ethiopian public universities.

1.4.2. Specific Objectives

This general objective can be broken down to three more specific objectives that would together achieve the overall goal of the research. The specific objectives of the research are:

- To investigate the current maturity level of information security implementation in Ethiopian public universities.
- To analysis the gaps exist between the current Information Security maturity level and expected level of maturity.
- To determine and analyze the uppermost and lowermost maturity scored Information Security Practice assessment areas.
- To indicate potential future improvements of information security in the sector.
- To draw conclusions and forward recommendations for further study.

1.5. Significance of the Study

The relevance of this research work is significantly important to the Ethiopian university sector. The proper interpretation of this research findings benefits to comprehensive and insightful examination of the current status and issues facing information security practitioners in Ethiopian universities. The study results could be used as a baseline knowledge on information security management in Ethiopian universities besides brings a step up in further in placing security at level where all Ethiopian universities have participated in an improved understanding and awareness of security as an increasingly prominent them in operations. The research result enables to improve the current understanding of information security issues and reinforces the suitability of information security as a strategically important business function for universities. In general, universities can utilize the research result to structure their information security management and identify major gaps in their current performance which can be mitigated.

1.6. Research Scope

The research is specific to the management of information security with in Ethiopian public university sector by looking some selected sample universities. The survey scope is limited to some selected universities, due to the time limit concern. The study is based on the information security perspectives and Limited to assess the current maturity level of information security management control, and analysis the maturity results to give recommendations for future improvements.

1.7. Limitations of the study

In the process of conducting the study, the researcher has encountered some constraints. One of the main limitations of this study was the lack of prior research studies on the specific subject matter and sector of the study. The lack of prior research studies in the subject matter affects this research in giving strong justifications. Though, this study presents an important opportunity for other researchers interested in the subject to explore Information Security from other perspectives. The other limitation is that, due to financial and time constraints the research covers only sampled universities. The result of the research would be more inclusive if it covers the entire public universities in Ethiopia and also increase the participant of the study by involving the large end users.

1.8. Thesis Layout

As presented below on figure 1, this thesis report is organized into six chapters which are also highlighted as follow:

Chapter 1: Chapter one of this study provide some background to explains the basis behind the study and proceeds with the formulation of the research problem followed with the research questions.

Chapter 2: chapter two presents a literature review relating to Information security management. Under this chapter a basic conceptual literatures and related works are reviewed

Chapter 3: Chapter three of this study presents the conceptual framework used in the research. Under this chapter, a conceptual framework is proposed conceptualizing the main dimensions for the study.

Chapter 4: This chapter provides the research methodology, research design, research data, data collection research population and sample.

Chapter 5: Chapter five of this study present the qualitative and quantitative data of the study along with the analysis, discusses and answering research question.

Chapter 6: This chapter is about conclusion, recommendations and suggestion for future works.

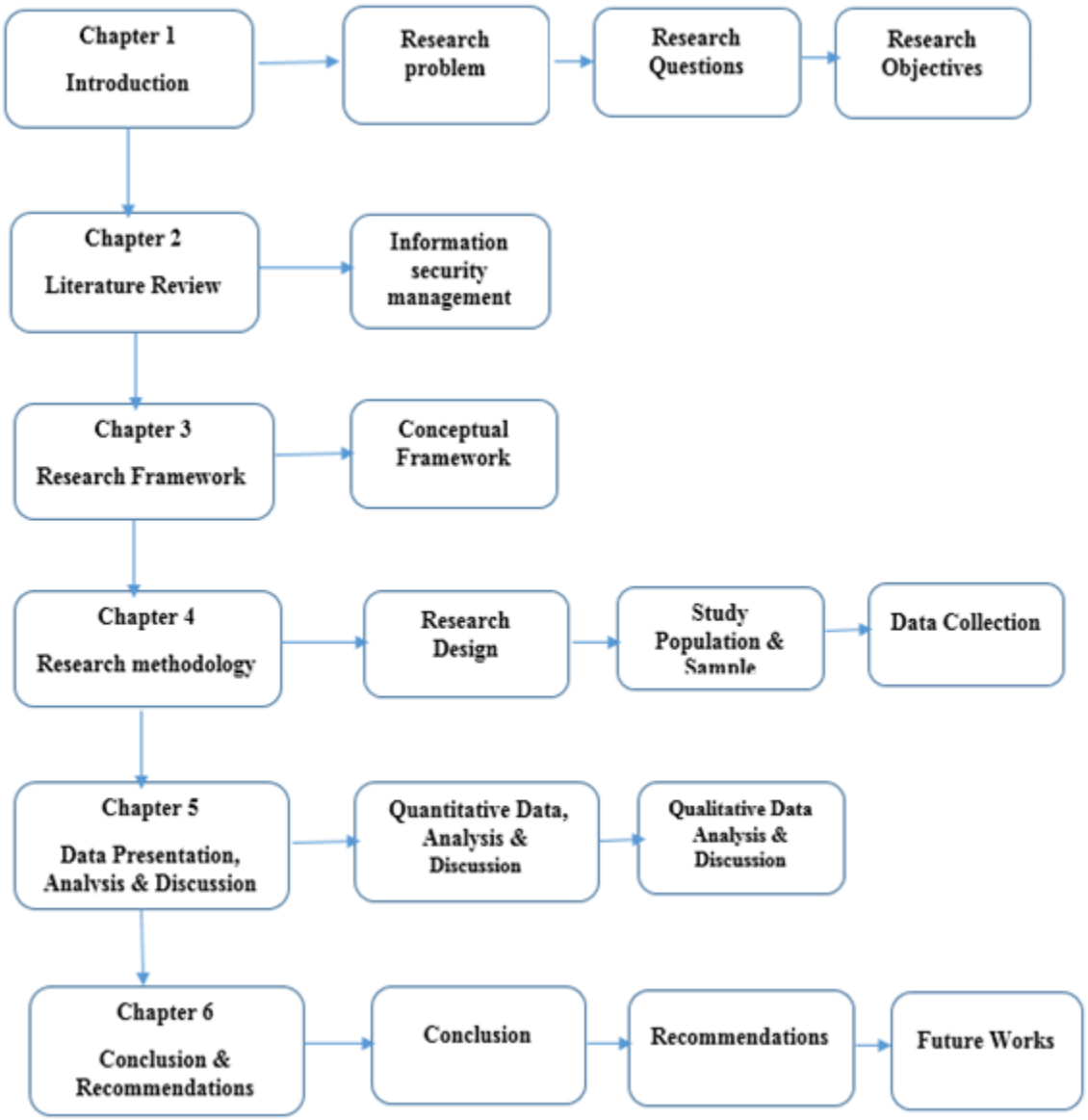

Figure 1: Structure of the Thesis

CHAPTER TWO: LITERATURE REVIEW

Under this chapter, a basic conceptual literatures and related works are reviewed. For the conceptual review, the following topic are presented; Information security, A short Historical Perspective to Information Security, Basic Information Security concept including CIA Triad, Information security threats, Information Security Management, Information Security Management System, ISO Information Security Management Standard and, Information Security in University Environment. In addition, related works are reviewed and presented.

2.1. Information Security

There are different forms of security for companies such as: Information security, operations security, production security, personnel security, computer security and so on. Information security describes activities that relate to the protection of information and information infrastructure assets against the risks of loss, misuse, disclosure or damage, responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage. Information security in an organization has a set of strategies for handling the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information asset (Mehdi , Hamid , & Hashem , 2012).

An information asset is stated as a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively (NIST, 2012). Information assets have recognizable and manageable value, risk, content and lifecycles. For example, a database of contacts is a clear example of a single information asset. Each entry in the database does not need to be treated individually; the collection of pieces of data can therefore be considered one information asset. Information assets should be grouped and considered depending on their business needs not on their technology requirements. Each asset may contain individual items that need different technology solutions to address the same business need and also Assets can contain other assets (Lenka & Roland , 2012).

Information is created and processed by employees, contractors and third-party users also known as Information users within business processes using applications and tools which are hosted in the IT infrastructure. As shown on the figure 2 below, consequently four areas need to be taken into account when implementing Information security (Ladan, Yari, & Khodabandeh, 2006).

- Information users: how people handle Information and use tools and applications properly to protect Information.
- Business processes: how Information security is embedded within working practices.
- Applications: how well they are developed to ensure the protection of Information stored and processed.
- Infrastructure: how well it provides sufficient capacities and adequate protection of Information and applications against unauthorized access and modification.

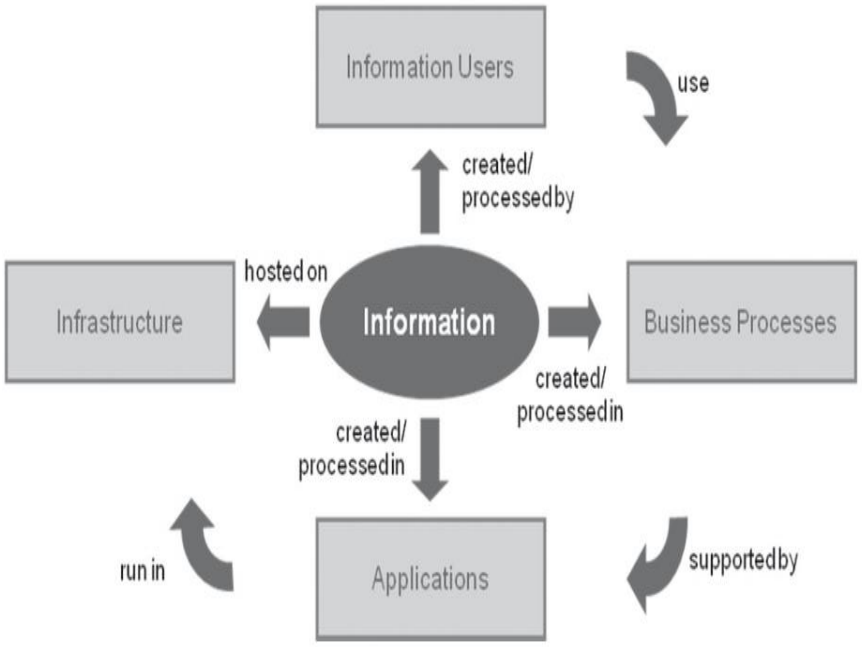

Figure 2: Aspects of the information processing

Source: Lenka & Roland (2012, p.12).

2.1.1. Short Historical Perspective to Information Security

The history of information security begins with computer security. The need for computer security that is, the need to secure physical locations, hardware, and software from threats arose during World War II when the first mainframes, developed to aid computations for communication code breaking, were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards (Candiwan, Puspita , & Nadiihaq , 2016).

Information security governance has been characterized as the fourth wave of security management. The first wave was technical in nature, the second wave was managerial, the third wave was institutional, and the fourth wave is about governance (Salahuddin , 2011). Accordingly, these are the four waves that are described in detail below on figure 3.

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

Figure 3: The ISMS Waves description and issues

Source: Salahuddin (2011, p.16).

2.1.2. Information Assets

Information plays a crucial role in today's organizations. It is seen as a valuable component, but few organizations have actually realized the full potential of their information assets. Information located in different parts of the organizations are often believed to be of huge value. Although they actually don't have any measurable financial attributes. Knowing the actual value of the information assets within organizations can lead to a better understanding of the more valuable and less valuable information. In order to qualify as asset information should have the following characteristics. It should have service potential or future economic benefits. It should be controlled by the organization and is the results of past transactions. Information meets all these requirements (Wilco, 2007). According to Daniel and Peter (1999), The followings are the different attributes of information:

- Information is expandable, it increases with use.
- Information is compressible, able to be summarized.
- Information can substitute for other resources.
- Information is transportable virtually instantaneously.
- Information is diffusive, tending to leak from the straightjacket of secrecy and control, and the more it leaks the more there is.
- Information is sharable, not exchangeable. It can be given away and retained at the same time.
- Information is human. It exists only through human perception.

Information is used to gain competitive advantage over competitors by enabling delivery of cheaper or more highly differentiated products. Information gives an added value and substitute for labor or capital investment. Information is also no longer seen as a cost-based activity, an activity to support other activities. Currently information is seen as an important source of value creation It is important that managers understand the role and impact of information on the organization. Whereas information can add value to products and services as well as improve quality of decision-making and reduce risks. The value of information is not a function of the information itself, but rather of measurable attributes of the information (Wilco, 2007).

Information satisfies the definition of an asset much better than employees or customers, which are also commonly referred to in the literature as assets. Employees and customers result in service potential and future economic benefits but are not owned by the company if employees were to resign or customers to change suppliers, the company would lose the benefits without compensation. Information is a non-physical or intangible asset. However, it is the service potential and economic benefits, not the physical form of an object, which is relevant in assessing whether an asset exists (Daniel & Peter, 1999).

2.1.3. CIA Triad of Information security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The three categories that are used to classify information security risks are confidentiality, integrity, and accessibility or availability of information (Deborah , Pamela , Linda , & Ronald , 2004).According to Sattarova and Tao (2007), the three major facets that are used to classify information security as the preservation of information are confidentiality, integrity, and accessibility or availability of information. protection of the Confidentiality, Integrity and Availability of data, also known as the CIA Triad and described as below:

- Confidentiality: the term used to prevent the disclosure of information to unauthorized individuals or systems. It assurance that information is shared only among authorized persons or organizations.
- Integrity: means that data cannot be modified without authorization. It assurance that the information is authentic and complete.
- Availability: information must be available when it is needed. This means that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Figure 4: Information Security Components (CIA Triad)

Source: Sattarova and Tao (2007, p.18).

As it is shown above on figure 4, Information Systems are decomposed in three main portions, hardware, software and communications with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: Physical, personal and organizational. Essentially, procedures or policies that are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations (Sattarova & Tao, 2007).

Information security involves making information accessible to those who need the information, while maintaining integrity and confidentiality (Deborah , Pamela , Linda , & Ronald , 2004). According to Tim (2007), these major distinct feature or elements of information security are guaranteeing the confidentiality, integrity and availability of information (referred to as the 'CIA' model of security). The confidentiality, integrity and availability of security is a relatively commonly accepted model, whereby security can be viewed as involving a process to provide information with the CIA principles. Until recently, the CIA model has been considered the 'cornerstone' of security. However, increasingly it is considered deficient in taking into account many of the other important aspects of security.

2.1.4. Information security threats

A threat is a potential cause of an unwanted incident that may harm to a system or organization (Pavlov & Karakaneva , 2011).Information security damages can range from small losses to entire information system destruction. Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant losses. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge (Mouna , Latifa , & Anis , 2014).

The development of Information and Communication Technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats. In fact, their information becomes exposed to cyber-attacks and their resulting damages (Mouna , Latifa , & Anis , 2014). Threats come from different sources, some common threats to attack systems are: (Ateeq , 2012).

- Virus Threats: A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user.
- Spyware Threats: A serious computer security threat, spyware is any program that monitors online activities or installs programs without owner's consent for profit or to capture personal information.
- Hackers: Hackers are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information as a form of cyber-terrorism.
- Viral Web Sites: Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites and are often made to look like well-known web sites and can have similar web addresses to the sites they are imitating.
- Spyware, Adware and Advertising Trojans: Spyware, Adware and Advertising Trojans are often installed with other programs, usually without owner's knowledge.

Based on the identified assets and asset types, the administrators have to identify and describe threats. Threat identification and description are used containing the following information (Wolfgang , Stefan , & Michael , 2012).

- Actor: The trigger or cause of a threat or damage occurring.
- Threat type: Allow the categorization of threats, e.g., malicious intent, accident or error, failure of hardware or software component used.
- Event: Short description of the threat event itself, also based on a category like disclosure of critical information, service interruption, unauthorized modification etc.
- Asset: The threat's description should contain information about the affected assets, e.g., the service infrastructure, the information or application.
- Time: This element can be used to describe further details about the threat's duration, the time the threat event occurs, or the time needed to detect security-related events.

2.2. Information Security Management

Information Security Management characterizes the process of personnel leading and directing all or part of an organization through the deployment and manipulation of resources (human, capital, natural, intellectual or intangible. It is an iterative process with feedback and continuous improvement, which consists of several processes that started with Identify and specify security requirements and will be continued to meet these needs with the required strategies and measuring results to improve information security management. It also consists of various aspects, which includes information security policy, risk analysis and management. The main task of information security management is to give confidence that, the security requirements that have been imposed on the system are adequate to protect data and resources. Another task is to ensure that information security management system is working somehow to meet the security needs and reports important deviations in security (Mehdi , Hamid , & Hashem , 2012).

Information security management is a set of managerial activities that aims to protect information assets and secure framework within the organization in which information systems are working. It labels controls that an organization needs to implement to ensure that it is rationally managing risks. The reason for managing risk in an organization is to protect the mission and assets of the organization. Information Security Management always correlates to

the implementation of an Information Security Management Systems (Pavlov & Karakaneva , 2011). This means that any kind of management within an organization, which deals with security-related issues, should incorporate an Information Security Management System (ISMS) in order to secure business information and to sustain the information environment.

2.2.1. Information Security Management System

Since information is growing faster than in the previous decades, there is a need to safeguard and manage that information efficiently and effectively in order to make it useful. From big corporations to small businesses, non-profit organizations and governments, organizations need to safeguard and secure their information (Bertrand , 2012).

Since information is growing faster than in the previous decades, there is a need to safeguard and manage that information efficiently and effectively in order to make it useful. From big corporations to small businesses, non-profit organizations and governments, organizations need to safeguard and secure their information by implementing information security management systems (Bertrand, 2012).

An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. ISMS encompass people, processes and IT systems. It also ensures the safety and reliability of the information, and to enhance the organization’s information security level of managerial, technical, and physical safeguards. The primary purpose of ISMS is concerned with the way, process or method in which information security is managed from the organizational perspective (Azah & Norizan , 2010).

A management system embraces all the policies pertaining to supervision and management for the purpose of achieving the institution's objectives. The part of the management system dealing with information security is referred to as the information security management system (ISMS). The ISMS specify the instruments and methods that the management should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security. As shown below on figure6, ISMS involve the following

essential components which are Management principles, Resources, Personnel and Information security process. In Information security process, Policy for information security in which the information security objectives and strategies for their implementation are documented, Information security concept and Information security organization (BSI- standard 100, 2008).

Figure 5: Components of an information security management system (ISMS)

Source: BSI- standard 100 (2008, p.14).

According to Tim (2007), an Information Security Management System (ISMS) provides a management framework which the organization can reference and is designed to meet the needs of the individual requirements of each organization. In respond to the requirements in security area was created special standards for ISMS. Information Security Management Systems are in effect, an organizational framework for the operation of information security. An ISMS should reference all the necessary required areas of governance for information security and include the use of an appropriate mix of policies, standards, guidelines, codes of practice and technical controls.

2.2.2. ISO Information Security Management Standard

According to Mark (2013), the four listed below are components of security documentation which are policies, standards, procedures, and guidelines. Together, these form the complete definition of a complete security program.

- Policy: policy is a high-level statement of requirements. It is the primary way in which management's expectations for security are provided to the builders, installers, maintainers and users of organizational information systems.
- Standards: It specifies how to configure devices, how to install and configure software, and how to use computer systems and other organizational assets, to be compliant with the intentions of the policy.
- Procedures: It specifies the step-by-step instructions to perform various tasks in accordance with policies and standard.
- Guidelines: These are advice about how to achieve the goals of the security policy, but they are suggestions, not rules. They are an important communication tool to let people know how to follow the policy guidance, it conveys best practices for using technology systems or behaving according to management's preferences

There is an ever-growing list of different number of standards for the management of information security and collections of best practice measures were developed and established. These standards of best practice and frameworks Published that can be used by organizations for comprehensive guide to identifying information security risks and implement appropriate information security management controls. National standards like NIST SP 800 series and the IT security guidelines which are the most important standards for the development and operation of an ISMS includes the ISO 270xx, and COBIT (Knut , Ricardo , Srdan , Knud , & Vladimir , 2016). In this study the ISO27 K family of standards is discussed and presented below.

2.2.2.1. ISO 27 K family of standards

Security standards can be used as guideline or framework to develop and maintain an adequate information security management system (ISMS). The ISO/IEC 27000-series also known as the 'ISMS Family of Standards' or 'ISO27k' encompasses information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC). In answer to the requirements in security area was created special standards for ISMS. Some of the Published editions of ISO/IEC 27000 series are listed following (Pavlov & Karakaneva , 2011).

- ISO/IEC 27000 – Information security management systems. Overview and vocabulary

- ISO/IEC 27001 – Information security management systems. Requirements
- ISO/IEC 27002 – Code of practice for information security management
- ISO/IEC 27003 – Information security management system implementation guidance
- ISO/IEC 27004 – Information security management. Measurement
- ISO/IEC 27005 – Information security risk management
- ISO/IEC 27006 – Requirements for bodies providing audit and certification of information security management systems.

The existence of the ISO 27000 to ISO 27002 standards can be traced back to 1993 as shown on figure 7. ISO 27001 formed the foundation for the ISO 27Kfamily of standards, which encompass various standards for information security. In 2007 the old ISO 17799standard was assigned to the ISO 27 K family as ISO27002. In 2009 ISO 27000 was issued to provide an overview, introduction and explanation of terminology with the title "IT Security Techniques Information security management systems Overview and Vocabulary" .ISO/IEC 27001:2013 is an information security standard that was published in September 2013. It supersedes ISO/IEC 27001:2005. For the protection of the information and information systems the standards ISO 27000, ISO 27001 and ISO 27002 provide control objectives, specific controls, requirements and guidelines, with which the company can achieve adequate information security. (Georg, 2013).

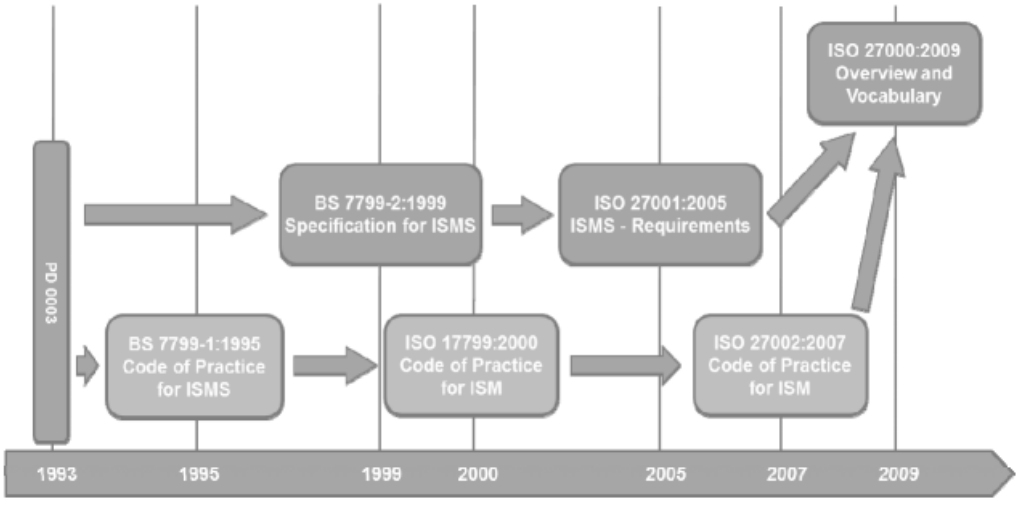

Figure 6:: Development of standards ISO 27000, ISO 27001, and ISO 27002

Source: Georg (2013, p.95).

Information security systems are often regarded by organizations as simple checklists or policies and procedures that deny them a lot of things, far from the way they do their normal business. By sticking to these beliefs, organizations prevent themselves from properly building an ISMS (Information Security Management System) and achieving its full potential, either in operational and financial performance, or marketing reputation. Fortunately, there are many frameworks on the market that can help organizations to handle this situation, among them being ISO 27001:2013. ISO 27001: 2013 ISM standard provides a model and guidelines to organization for implementing, operating, monitoring, reviewing, managing and improving an information security management by introducing as of controls to an acceptable level of protection. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature (ISO/IEC 27001, 2013).

ISO/IEC 27001

The ISO 27001 standard was published in 2005 under the title Information technology—Security techniques Information security management systems Requirements. ISO/IEC 27001 standard specifies requirements for the design and implementation of an appropriate Information Security Management System (ISMS) in an organization, ensuring that adequate and proportionate controls are selected to protect information assets and to give confidence to interested parties. This standard is used throughout the world by organizations, both commercial and government, as the basis for the management of the organization's policy and implementation of information security. It is being used by small, medium and large organizations across a diverse range of business sectors (Razieh & Nasser , 2012).

The ISO/IEC 27001 ISMS standard adopts the well-known PDCA process approach as illustrated infigure8. The PDCA approach is also called a continuous improvement since the management system is regularly monitored and reviewed to check whether the controls to

manage the risks are still effective and if they are not, then improved controls need to be implemented. The PDCA cycle has these four phases (BSI- standard 100, 2008).

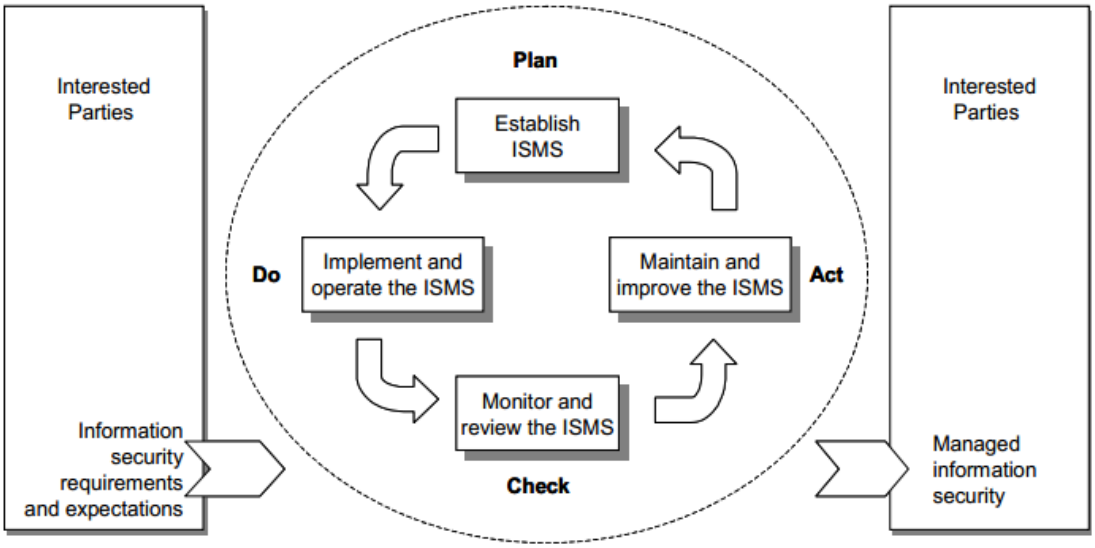

Figure 7: PDCA model applied to ISMS processes

Source: ISO/IEC 27001 (2005, p.6).

The management of information security is based on the so called “Plan-Do-Check-Act” model (four phases), introduced by ISO/IEC 27001. The PDCA cycle is a globally recognized management system methodology that is used across various business management systems, but its use is both compulsory and highly beneficial within ISO 27001. The “Plan-Do-Check-Act” cycle (PDCA) which can be described as follows: (Pavlov & Karakaneva , 2011).

- 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.

ISO/IEC 27002

The focal point of ISO 27001 is the requirement for planning, implementation, operation and continuous monitoring and improving of a process-oriented ISMS. The codified requirements in ISO 27001 are expanded and explained in ISO 27002 in the form of a guideline. The continuing development of ISO27002 is based on the presentation of ISO 27001. In annex A of the standard a total of 39 control objectives and 134 measures for security management are listed and thus expressly stipulated. The control objectives are listed below, subdivided by domains in to 11. These are described further and detailed in the ISO 27002 standard (Georg, 2013).

1. Security policy: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
2. Organization of information security: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
3. Asset management: To achieve and maintain appropriate protection of organizational assets and to ensure that information receives an appropriate level of protection.
4. Human resources security: To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
5. Physical and environmental security: To prevent unauthorized physical access, damage and interference to organization's premises and information.
6. Communications and operations management: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
7. Access control: To control access to information by preventing unauthorized access to networked services, operating systems and information held in application systems.
8. Information systems acquisition, development and maintenance: To ensure that security is an integral part of information systems and also to prevent errors, loss, unauthorized modification or misuse of information in applications.

9. Information security incident management: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
10. Business continuity management: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
11. Compliance: To ensure compliance of systems with organizational security policies and standards and to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

2.3. Information Security in University Environment

Universities have adopted information systems and the related technologies so as to gain a competitive edge. In this era effective control of operations and strong strategies are associated with management of quality information. The aspect of readily available information means that universities are affected by their dependence on information and technology resources, systems and the underlying structures that form the basis for this technologies and systems. In universities, reliance on information systems is evident on activities related to creating, using and sharing of information in teaching, learning, research and development and when marketing the university through its websites. It's evident that the amount of intellectual property generated by universities and importance of university information is extensive (Bichanga & Obara , 2014).

The extensive autonomy of organizational units in Higher Education Institutes (HEIs) is often seen as a challenge for IT governance and security management is no exception. Management commitment to information security is one of the first important building blocks, and therefore many HEIs that, for example, established a chief information officer (CIO) position at the level of a vice president decide to introduce the role of a chief information security officer (CISO) either as a dual role for the CIO or appoint, e.g., the head of the IT department or a security expert in a leading position as CISO with direct reporting to the CIO (Wolfgang , Stefan , & Michael , 2012).

There are many technical solutions to help protect the information assets of an organization, the risk of information leakage, modification or destruction cannot be completely eliminated. As this may incur great losses, information security is essential to any organization which counts information assets as critical to their business operation. This is especially important for government and public bodies because the adverse impacts are much greater than that of other organizations. Similarly, for a higher education institution where a large amount of student information is hosted student administrative systems, learning management systems and platforms, any information leakage or loss would have large impacts (Simon , 2014).

2.4. Related Studies

An Exploratory Analysis research by Tim (2007), is conducted on Information Security Management in Australian Universities. The purpose of the research was to undertake an exploratory analysis of information security management in Australian universities in order to understand the status, and identify issues, barriers and enablers to security management in universities. This research undertook a qualitative based exploratory analysis of information security management in Australian universities. The research aims to a comprehensive and insightful examination of the status, issues and challenges facing information security practitioners in Australian universities. The research findings culminated in the development of a Security Practitioner's Management Model. The model seeks to provide a way to think about the fundamental challenges faced by the security practitioner in progressing security implementation within Australian universities. An essential aim of the model was to assist security practitioners to successfully implement and progress information security in the Australian university environment. The results of this research indicate that universities face a number of challenges in relation to implementing information security in time of the study environment. The study recommends that future research would be well-placed to focus on benchmarking information security management within the university sector.

Another study was taken place by Lloyd (2012), on an Appraisal of Information Security Management at Chancellor College, University of Malawi". The aim of this research was to assess information security management at Chancellor College. In this study a deep look at the information security practices and experiences at Chancellor College in light of International

Standards for information security as well as other prominent publications are used to define the baseline requirements for information security. The research choice of methodology was qualitative research. It transpires that even in the midst of sufficient finances, information security can still go awry. The study concludes that major challenges exposed by other studies of both universities and the corporate institutions worldwide namely policy issues, academic freedom, organization culture, user awareness, staffing, top management support, ICT infrastructure are the same challenges that Chancellor College is facing. The researcher also recommended a further research on Server and Network configurations, and System Development Practices and their impact on security.

A study by Candiwan, et al. (2016), is conducted on Assessment of Information Security Management on Indonesian Higher Education Institutions. It is stated that many security breaches had happened on universities in Indonesia in many forms, such as penetration of the official website, website defense and penetration to academic system to change scores. The purpose of the reach was to capture the implementation of information security management in some higher education institutions in Indonesia and not to generalize the condition of all institutions. The paper used a descriptive approach to explore the maturity level of particular items in main clauses and controls of ISO 27001:2013. The result forms the research shows that average score of maturity level of information security management is still limited on initiatives from its IT organization. It is also mentioned that; some controls are repeatable without adequate planning and documentation. The research is preliminary for further research to build a framework for information security management in higher education institutes and also recommend for the study bout influence factors in implementing information security and analysis of Information risk.

A Gap Analysis Between Common Practices and Industry Best Practices research by Philip (2013), is conducted on Information Security Management Systems in Public Universities in Kenya. This research is concerned with issues regarding information security management in public universities in Kenya. The main aim of this research was to investigate status of information security management practices in Kenyan public universities. To help information security practitioners in these institutions to implement effective information security

management systems, a framework for information security management grounded on industry best practice guidelines and recommendations in information security management was proposed. The framework guided a comprehensive study to understand the information security control environment in public universities in Kenya. A descriptive survey targeting information security professionals and users of information systems was carried out. The study findings indicate that the information security control environment in public universities is inadequate. The main barriers to information security include enforcement of policies, lack of senior management support and lack of resources. the main issues, barriers and factors that influence information security management have been highlighted with recommendations about how to address them to secure information assets.

A research looked by Bichanga and Obara (2014), into the challenges facing information systems security management in higher learning institutions in Kenya. The research looked into the challenges facing information systems security management in higher learning institutions. The study was guided by understanding the major challenges facing Information Systems Security Management and establishing the extent of the use of Information Systems Security Management in higher learning institutions. The study used descriptive based survey study and found out that system vulnerability, computer crime and abuse, environmental security and financial backing/security are key challenges institutions of higher learning and experiencing in the management of their information systems. The study recommends the implementation of new policies and procedures to guide information system security. Programs for monitoring and evaluating information systems security in relation to performance indicators should be put in place. Institutions should invest heavily in developing their staff through training programs.

A study by Rosmiati and Yudi (2016) with a title "A Maturity Level Framework for Measurement of Information Security Performance" is conducted. This research was conducted to find out the level of information security in organization to give recommendations improvements in information security management at XYZ company. This research used the ISO 27001 by involving the entire clause that exists in ISO 27001 checklist. The source of the data used in this study was a detailed questionnaire and interview. The results showed maturity level of information security in the Office of the Bureau of information technology is at level 2. The

value of the gap between the value of the maturity level of the current and expected level of maturity value is 2.79. Results of the questionnaire management to obtain an average value for all of the clauses is 2:21 range of 0 to 5. Recommendations for improvement are given requires an understanding of the company and also required coordination with the internal company.

A study by Kelemie (2013), was conducted on Information Security Management Framework for Banking Industry in Ethiopia. The objective of this study was to assess the Information Security Management (ISM) practices of banking sector, and to propose and develop ISM Framework. In this study, attempts were done to examine and compare the available ISM frameworks and best practices. The research combines ISO audit checklist and researcher's own experience to assess the information systems security practices in banking industry. For the study, both qualitative and quantitative research approach were used. The Data were collected via questionnaire survey, document analysis, and interviews. The study results show that surveyed banks are at diverse states in managing the security of their information systems. Moreover, they all are found to be at low level of ISM practice. A framework for ISM is developed and evaluated. The framework shows how banks identify their security requirements and select controls. Sixteen main ISM domains are identified and in turn these ISM domains are classified under three categories viz. Administrative, Technical, and Physical & Environmental security. Further, some of areas that require policies and procedures are identified.

Title, Author Year	Objective of the study	Research Type or Methodologies	Findings	Recommendation
Information security management in Australian universities: An Exploratory Analysis, (Tim , 2007).	To undertake an exploratory analysis of information security management in Australian universities in order to understand the current status, and identify issues, barriers and enablers to security management in universities.	The research applied a qualitative method to undertake an exploratory investigation.	The research findings culminated in the development of a Security Practitioner's Management Model.	The study recommends that future research would be well-placed to focus on benchmarking information security management within the university sector.
Appraisal of Information Security Management at Chancellor College, University of Malawi, (Lloyd , 2012).	The aim of this research was to assess information security management at Chancellor College.	Qualitative research	Major challenges exposed namely, policy issues, academic freedom, organization culture, user awareness, staffing, top management support, ICT infrastructure are the same challenges that Chancellor College is facing.	Further research on Server and Network configurations, and System Development Practices and their impact on security.

Assessment of Information Security Management on Indonesian Higher Education Institutions, (Candiwan, Puspita , & Nadiihaq , 2016).	To capture the implementation of ISM in some higher education institution in Indonesia.	Descriptive Approach	Implementation of ISM is still limited on initiatives from its IT organization.	To build a framework for ISM in higher education institutions and Influence factors in implementing information security and analysis of information risk
Information Security Management Systems in Public Universities in Kenya: A Gap Analysis Between Common Practices and Industry Best Practices (Philip , 2013).	The aim of this research was to investigate status of information security management practices in Kenyan public universities.	Descriptive survey	Information security control environment in public universities is inadequate to deal effectively with information security threats.	Recommends further research to get insightful information regarding information security policy structure and content.
Challenges facing information systems security management in higher learning institutions in Kenya, (Bichanga & Obara , 2014).	To look into the challenges facing information systems security management in higher learning institutions.	Descriptive survey	System vulnerability, computer crime and abuse, environmental security and financial backing/security are key challenges institutions of higher learning.	Institutions should invest heavily in developing their staff through training programs to further develop staff skills and abilities on information systems security issues.

A Maturity Level Framework for Measurement of Information Security Performance (Rosmiati & Yudi , 2016)	The aim of this research was to find out the level of information security in XYZ company.	Qualitative research method.	Results of the questionnaire management to obtain an average value for all of the clauses is 2:21 range of 0 to 5.	The study recommends on the improvement of weak controls.
Information Security Management Framework for Banking Industry in Ethiopia. (Kelemie , 2013).	The objective of this study was to assess the Information Security Management (ISM) practices of banking sector, and to propose and develop ISM Framework.	Both qualitative and quantitative research approach were used.	The study results show that surveyed banks are at diverse states in managing the security of their information systems. Moreover, they all are found to be at low level of ISM practice.	Aspects of ISM that are beyond the scope of the research are recommended for future research in require policies and procedures.

Table 1: Summary of Reviewed Related Studies

CHAPTER THREE: THE RESEARCH FRAMEWORK

Firstly, it is important to understand what a 'framework' is, within the context of research. According to Sitwala (2014), Research Framework is defined as a structure that provides guidance for the researcher as study questions are fine-tuned, methods for measuring variables are selected and analyses are planned.

Under this chapter, a conceptual framework is proposed conceptualizing the main dimensions for Information security management in public universities in Ethiopia. It is based on information security management best practice and guidelines as recommended in various standards, guidelines and literature by information security researchers and practitioners. The proposed research framework served as a guide to the data collection process including the development of research questionnaires and interview outline, which are discussed under chapter four.

3.1. Research conceptual framework

In order to study the information security management practice in Ethiopian public universities which is required for an effective information security management, a pre-defined conceptual framework is proposed. From a theoretical perspective this study is a contextual analysis, as the intention is to find out the maturity level of information security in Ethiopian public universities.

The research framework is closely linked to the research questions. It is also aimed and designed to meet the study objective and answer the following research questions.

i. What is the current maturity level of information security implementation in Ethiopian public universities sector?
ii. What are the uppermost and lowermost maturity scored information security controls in Ethiopian public universities?
iii. How could potential improvements in information security be achieved in Ethiopian public universities?

The Research Conceptual Framework is concerned on the assessment or measurement of the maturity level of Information security implementation in the Ethiopian public universities. The output of analyzing the Conceptual Framework helps to answer the research questions of the study. The organization of the Conceptual Framework is discussed in detail below under sub topics of this chapter and Supported with literature that has been highlighted under Chapter 2 (literature review) part of the study. Also, the results and analyzed based on research framework is presented under later chapter along with the methodology used for the analysis.

The research also adopted the following concepts in conceptualizing the research framework.

- The objective of an information security is to protect the integrity, confidentiality and availability of an organization's information (Mehdi , Hamid , & Hashem , 2012).
- The effectiveness of Information Security Management depends on the implementation strength of security controls (Candiwan, Puspita , & Nadiihaq , 2016).
- One of the tools of measurement of the performance of system information is a model of maturity level (Endang & Imam , 2018).
- Maturity assessments are a proven way to assess, communicate, manage information security programs and even can lead to more effective IT governance (Christophe , 2016).

As it is mentioned above, the research framework is concerned on the assessment or measurement of the maturity level of ISM practice in the Ethiopian public universities. This assists to find out the level of information security implementation and to give improvement recommendations in information security management in the public university sector in Ethiopia. In order to do achieve this goal, the study is mainly grounded on ISO 27001: 2013 Standard and Systems Security Engineering Capability Maturity Model (SSE-CMM) Maturity level assessment model. This is because the ISO does not have the methods of assessment (Rosmiati & Yudi , 2016). In order to determine variables which are the information security practice assessment areas, the study mainly uses the ISO 27001:2013 by involving the entire clause that exists in ISO 27001 checklists which are presented in figure10.

As it shown in figure 10 below, the information security assessment areas are to be scaled on the 5 levels of the maturity model. Once the maturity level of the current process is set and the target of process maturity has been determined, then the gap between the current conditions and the targets to be achieved will be analyzed the identification of opportunities in the gap to be optimized.

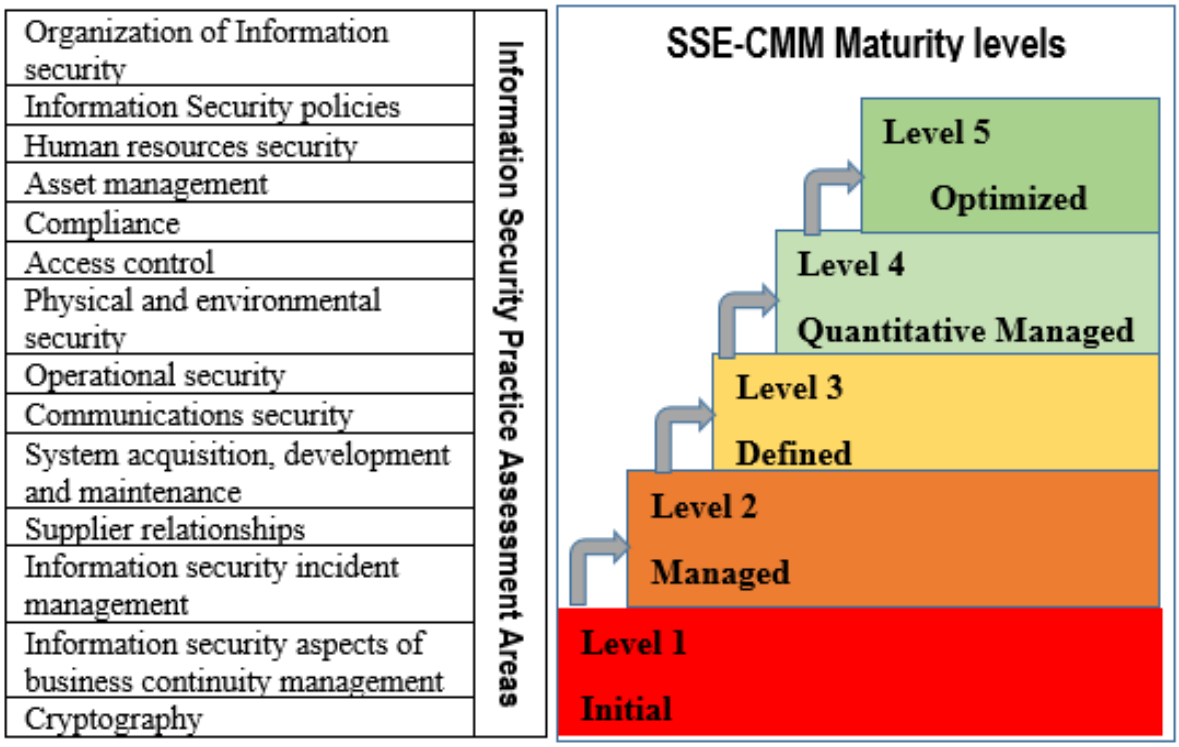

Figure 8: Research framework for Measuring the Maturity level of Information security

3.1.1. SSE-CMM

The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM is organized into two parts which are processes and maturity levels. The processes define what needs to be accomplished by the security engineering process, and the maturity levels categorize how well the process accomplishes its goals. The model's aim is to improve existing software development processes, but it can also be applied to other processes. The model is a standard metric for security engineering practices (SSE-CMM, 1991).

The measurement of maturity for each process-dimension pair is taken using a predefined maturity scale, which ranges from a maturity level of one to five. The maturity scale is uniformly applied to all of the measurements: for each process, for each dimension, determine a maturity level using the maturity scale. This approach is logical, repeatable, and reliable. SSE-CMM method used by giving the score assessment on each area of the process that selected between 0 to 5 for each process area (Christophe , 2016). The CMM maturity levels are:

- Level 0 indicates not all base practices are performed.
- Level 1 indicates all the base practices are performed but informally, meaning that there is no documentation, no standards and is done separately.
- Level 2 planned & tracked which indicates commitment planning process standards.
- Level 3 well defined meaning standard process has been run in accordance with the definition.
- Level 4 is controlled quantitatively, which means improved quality through monitoring of every process.
- Level 5 is improved constantly indicating the standard has been perfect and the focus to adapt to changes.

3.1.2. Maturity model

Maturity model is intended to determine the existence of the problem and how to determine the priority of improvement. Results of calculating the value of the maturity level is maturity index to obtain the level of maturity in accordance with table 2 shown below (Rosmiati & Yudi , 2016).

Maturity Index	Maturity Level
0 – 0.49	0 – Non-Existent
0.51 – 1.50	1 – Initial / Ad-hoc
1.51 – 2.50	2 – Repeatable but Intuitive
2.51 – 3.50	3 – Defined Process
3.51 – 4.50	4 – Managed and Measurable
4.51 – 5.00	5 - Optimized

Table 2: Maturity Level Assessment Criteria index

Source: Rosmiati and Yudi (2016, p.3).

Maturity model for management and control in the process of information system based on the evaluation methods of the Organization so that it can evaluated himself from level 0 (none) to level 5 (optimistic). Assessment of the ability and maturity of selected ISM Standard using maturity level, the assessment results show the maturity level of existing IT processes. Next will be determined maturity targets for each selected IT process, the maturity target of each process is the ideal condition that will be achieved in the definition of the desired maturity level, Descriptions measurement techniques are made by the nominal size to sort objects from the lowest to the highest, these measurements only give the order rank. Measurements were carried out directly from values that refers to the values of the exiting sorting in maturity models as show in table 3 (Rosmiati & Yudi , 2016).

Range	Descriptions
1 Initial	Company reactively perform application and implementation of information technology in accordance with the needs of existing sudden, without preceded by prior planning.
2 Repeatable	The Company has a pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency.
3 Define	The Company has had a formal and written standard operating procedures that have been socialized to all levels of management and employees to be obeyed and worked in daily activities.
4 Manage	The company has had a number of indicators or quantitative measures that serve as targets and objective performance of every application of information technology applications.
5 Optimized	The Company has implemented the information technology governance refers to "best practice"

Table 3: Maturity Level

Source: Rosmiati and Yudi (2016, p.3).

3.1.3. Information Security Practice Assessment Areas

As is it presented under the literature review part of this study, ISO 27000 series standard was reviewed from different studies researched by various authors in the past. Consequently, while selecting the Information Security Practice Assessment Areas of the study, the objectives of the assessment and the environment under which the assessment carried out is considered. As it is discussed under chapter 2 (literature review) part of the study, ISO/IEC27001 provides organizations with a structured approach to information security management to enable them to secure their information assets. The standard covers all types of organizations standard and tends to be generic and therefore the ISM best practices were selected on the basis of their applicability in institutions of higher learning (Razieh & Nasser , 2012).

ISO 27000 series is a family of IS management standards. It is the set of standards in this family that focuses on Information Systems Management (Rosmiati & Yudi , 2016). The organizational structure of ISO / IEC 27001 is divided into two major parts. The first part is called clause which is mandatory process Clause (Article) is a requirement that must be met if the organization implements ISMS using standard ISO/IEC 27001, whereas the second part is called Annex A. This security control Annex A is a reference document that is provided and can be used as a reference to determine what security controls (security control) that need to be implemented in the ISMS, which consists of 114 controls from 14 domains of security control clauses and 35 objectives in as shown in table (ISO/IEC 27001, 2005).

Many studies are undertaken by relying on ISO/IEC 27001 standard. To mention a study from the many reviewed relating studies under chapter two, the study by (Candiwan, Puspita , & Nadiihaq , 2016) for the Assessment of Information Security Management on Indonesian Higher Education Institutions which undertakes a descriptive approach to explore the maturity level of ISM implementation using items in main clauses and controls of ISO 27001:2013. Likewise, in determining the variables which are main key focus areas in which most information security management areas, this study primarily relied on the ISO 27001:2013 standard. This standard is adopted in order to assess the maturity level and capture the implementation of information security management in higher education institutions in Ethiopia. Based on the key focus areas or domains of ISO 27001:2013 standard shown in table 4, the research instruments are designed.

In general, the study focuses on the following key areas of Information security (Annex A.5-A.18) to assess or measure their implementation level using the maturity measuring model presented above on figure 10.

No. Annex	Domain of ISO 27001:2013	Number of objectives	Number of controls
A.5	Information security policies	1	2
A.6	Organization of information security	2	7
A.7	Human resources security	3	6
A.8	Asset management	3	10
A.9	Access control	4	12
A.10	Cryptography	1	2
A.11	Physical and environmental security	1	15
A.12	Operational security	7	14
A.13	Communications security	2	7
A.14	System acquisition, development and maintenance	3	13
A.15	Supplier relationships	2	5
A.16	Information security incident management	1	7
A.17	Information security aspects of business continuity management	2	4
A.18	Compliance	2	8
Total		35	114

Table 4: Domains, objectives and number of controls in Annex of ISO 27001:2013

Source: Candiwan, Puspita, and Nadiihaq (2016, p.3).

CHAPTER FOUR: RESEARCH METHODOLOGY

Under this chapter, details of the research methodology used in the study are discussed. It provides detail description on the activities which were essential for the completion of the research this includes; the general research design, Population of the Study, Research Sample, detailed description of methods used for data collection, and data analysis.

4.1. Research Design

There are three common approaches to conducting research which are quantitative, qualitative, and mixed methods and the researcher anticipates the type of data needed to respond to the research question (Carrie , 2007). To meet its objective and gather the required data, this research selected both Qualitative and Quantitative methods (A mixed method). As per (Bhawna & Gobind , 2015), A mixed methods research design is a procedure for collecting, analyzing, and "mixing" both quantitative and qualitative research and methods in a single study to understand a research problem. A mixed methods approach is one in which the researcher tends to base knowledge claims on pragmatic grounds

The mixed methods approach for research questions requiring both numerical and textural data (Carrie , 2007). A Quantitative approach is used to respond to research questions requiring numerical data (Carrie, 2007). In the case of this study A quantitative analysis is conducted through a survey questionnaire it helped to assess and identify the current maturity level of information security in public Ethiopian universities sector. On the other hand, the qualitative approach for research questions requiring textural data (Carrie , 2007). In this study the Qualitative approach was used to explore attitudes, get an in-depth opinion and experiences of respondents regarding to the subject matter and acquire data necessary in responding the research question.

As it is show below in figure 12, the research goes throw the, literature review, designing research framework and methodology, Preparing Research Instruments, pilot study, data collection/full assessment, data analysis, recommendation and Conclusion steps throw out the research process.

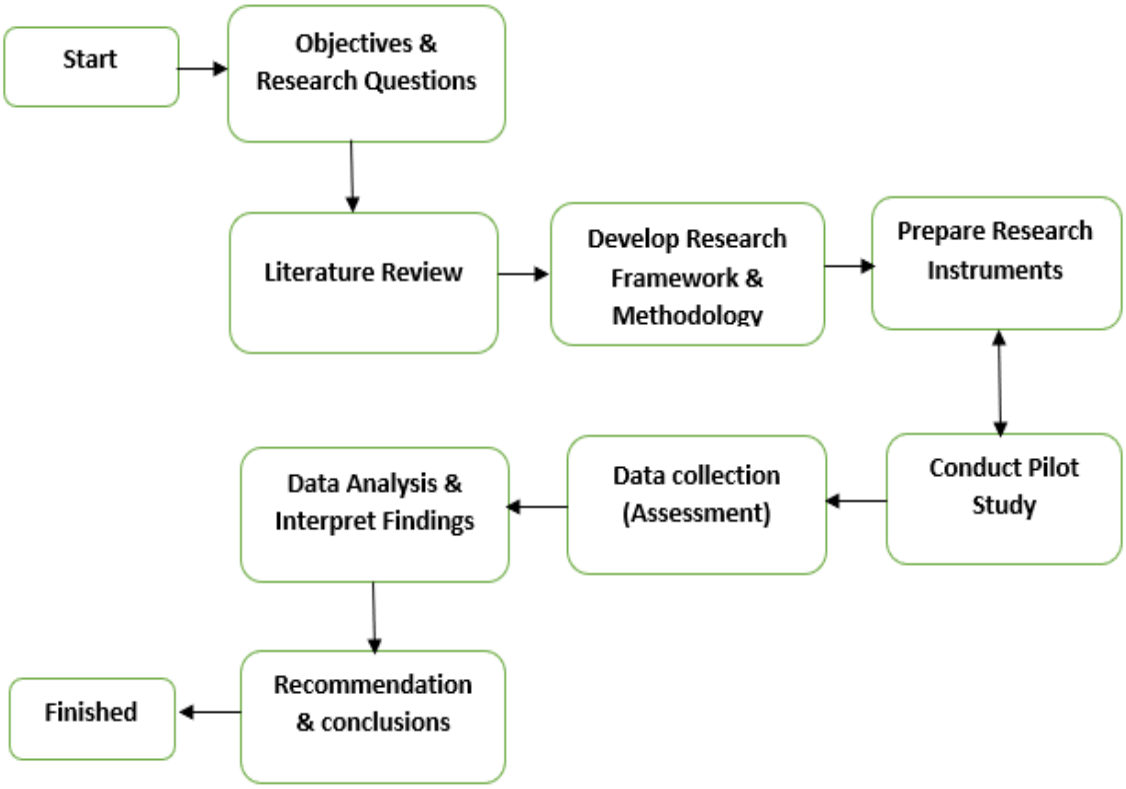

Figure 9: Research design and steps

4.2. Study Population

The population of this study contains the Ethiopian public universities. By the time of initiating the research, the accredited Public Universities in Ethiopia that are administered via the Ministry of Higher Education were 31. These universities are established and upgraded throw three phases, which as shown below in table 5. However, the number has grown after the government opened new 11 Universities by the late year 2017. The researcher assumes that the pioneer universities established in the sector, the more stable and experienced on the subject matter. Consequently, the recently opened 4th round generation universities are not included in the study.

As it is shown below in table 5, the nature of the universities existence is in generation-based strata. Meaning by the universities already created a stratum based on their establishment time and the moment of upgrade from college to university as it can also be seen from Appendix D in detail. This gives the above mentioned 31 universities to be clustered in to three generations. The

1st Generation universities consists 8 universities. The Second-generation universities strata consists 13 universities and the third-generation strata consist 10 universities. From theses total population sample universities for the study are selected.

No.	University	Generation
1	Addis Ababa University	1st Generation universities
2	Haramaya University	
3	Hawassa (Debub) University	
4	Jimma University	
5	Gonder University	
6	Bahir Dar University	
7	Arba Minch University	
8	Mekelle University	
9	Dilla University	2st Generation universities
10	Adama University	
11	MizanTepi University	
12	MadaWalabu University	
13	Semera University	
14	Debre Markos University	
15	Wollo University	
16	DebreBirhan University	
17	Aksum University	
18	WolaitaSodo University	
19	Dire Dawa University	
20	Wollega University	
21	Jijiga University	
22	Ambo University	3st Generation universities
23	Metu University	
24	Bule Hora University	
25	Addis Ababa Science and Technology University	
26	Debre Tabor University	
27	Woldiya University	
28	Asosa University	
29	Adigrat University	
30	Wachamo University	
31	Wolkite University	

Table 5: List of Accredited list of Public Universities in Ethiopia

Source: Federal Democratic Republic of Ethiopia Ministry of Higher Education (2010)

4.3. Research Sample

Sample is a portion of a population or universe (Ilker , Sulaiman , & Rukayya , 2015). The study used both Non-probability and probability sampling methods. From probability sampling methods, proportional stratified sampling is used to select universities among the formed generation-based stratums of public universities exist in Ethiopian context. In addition, from Non-probability sampling methods, purposive sampling is used to select the participant for the study.

As it is mention above, the universities already created a stratum based on their establishment time and the moment of upgrade from college to university. The formed stratums have an advantage for considering the age of the university. The criteria for selection of universities is based on these strata created regarding of the year of establishment and the moment of upgrade from college to university. From probability sampling method, proportional stratified sampling is used to select universities from these already formed generation-based stratums of universities exist in Ethiopian context. Thus, the 31 universities are categorized in to three generations. The 1st Generation universities consists 8 universities and 3 universities were selected. The Second-generation universities category contains 13 universities and 4 universities were selected proportionally. Whereas the third-generation strata consist 10 universities and 3 universities were selected. In total, from 31 universities 10 universities were proportional selected as sample for the study. This results the sample size to contain 32.25% of the total population. According to Gigi (2017), Stratified sampling might be preferred over simple random sampling when it is important to represent the overall population and to represent the key subgroups of the population, especially when the subgroups are small but distinguished in important ways. By using stratified sampling methods, a researcher can effectively assure that subgroups can be differentiated in the discussion of the research findings.

On the other hand, from Non-probability sampling method, purposive sampling was used to select the participant for the study. Purposive is the deliberate choice of a participant due to the qualities the participant possesses and based on their specialized insight or special perspective and experience (Ilker , Sulaiman , & Rukayya , 2015). This sampling method is used to select the one which is directly related to the subject matter.

In order to get representative and select respondent for the study, the researcher considered respondent knowledge and role in information security management in the universities. In order to generate questionnaires data, the research targeted on the ICT Directorate staffs of the sampled universities, which includes ICT Directors, ICT infrastructure unit mangers, System administrators, Network administrators and IT security experts who are professionals in the area of information security management are selected as a participant. ICT professionals are the people which directly involved with information security management relating tasks in the institutions. Respondent in this collection were in a position to give reliable information regarding information security status in their universities. The researcher therefore targeted these respondents from the ten sampled universities. Overall, the researcher targeted a projected sample of 120 respondents after conducting a preliminary study in acquiring the size of the selected 10 sample universities ICT Directorate staffs. Like wisely for the interview instrument, interviewees respondents are selected purposefully who are believed to be appropriate key informants for the study, these are information security professionals and at the management position which are IT Director or equivalent IT Security manager.

4.3.1. Overview of selected Universities

The Overview of the selected ten sample Higher education institute (HEI) is discussed below.

Addis Ababa University (HEI 01): Addis Ababa University (AAU), was established in 1950 as the University College of Addis Ababa and later in 1962 renamed as Haile Selassie I University. The University received its current name in 1975. Addis Ababa University is the oldest and the largest higher learning research institution in Ethiopia. Currently, it has fourteen campuses.

Hawassa University (HEI 03): Hawassa University (HU) was established in 2000. Since 1976 the colleges of HU had been operational starting with the College of Agriculture. The university was formed by merging three colleges in southern Ethiopia: Awassa College of Agriculture, Wondogenet College of Forestry and Dilla College of Teacher Education and Health Sciences**.**

Bahir Dar University (HEI 02): Bahir Dar University (BDU) was established by merging two former higher education institutions; namely the Bahir Dar Polytechnic and Bahir Dar Teachers' College. The Bahir Dar Polytechnic Institute, which has transformed itself into Technology and

Textile institutes, was established in 1963. Bahir Dar University is located in the city of Bahir Dar.

Adama University (HEI 04): Adama Science and Technology University (formerly known as Nazareth Technical College, Nazareth College of Technical Teachers Education, and Adama University). It is located in Adama, the capital city of Oromia regional state of Ethiopia. It was first established in 1993 and renamed as Adama Science and Technology University in 2011.

Samara University (HEI 05): Samara University (SU), Ethiopia, is a higher education institution located in the town of Samara, Afar Region. Officially accredited by the Ministry of Education (MOE), Ethiopia in 2008.

Wollega University (HEI 06): Wollega University is one of the public higher educational institutions in Ethiopia. It is established at Nekemte in 2007. The institution is one of the new Public Universities that was to be established under the University Capacity Building Program.

DebreBirhan University (HEI 07): DebreBerhan University (DBU) is one of thirteen new Universities which were established in 2007 by the Ethiopian government. It is located in Amhara Region, North Showa Zone, in the town of DebreBerhan.

Ambo University (HEI 08): Ambo University is a university in Ambo city, Ethiopia. The University was established in 2011 by the Ministry of Higher Education, Federal Democratic Republic of Ethiopia.

Addis Ababa Science and Technology University (HEI 09): Addis Ababa Science and Technology University, or AASTU, is one of the two Science and Technology Universities of Ethiopia. The main campus is located in Addis Ababa, Akaky Kaliti subcity.

Wolkite University (HEI 10): Wolkite University Founded in 2011 and Officially accredited and/or recognized by the Ministry of Education, Ethiopia. It is a public higher education institution located in the suburban setting of the medium-sized town of Welkite.

4.4. Data Collection

For conducting this research study, both primary and secondary data were used. Questionnaire and interview were used as primary data source besides to the analysis of written documents which is used as a secondary data Sources. These instruments are discussed below in detail.

4.4.1. Questionnaire

Questionnaires are prepared, organized and designed questions which are to be answered by respondents in the process of formulating general opinion about a phenomenon (Murtala , 2015). In the case of this study, a questionnaire is used as a main data collection method to collect the research quantitative data. The questionnaires (Appendix B) consisted of two parts containing a combination of both open-ended and closed-ended questions. The closed-ended questions had exclusive responses of “Yes”, “No” or “Don’t know” responses. While evaluating the controls, a five-point scales, "1" Very low, "2" Low, "3" Moderate, "4" High, "5" Very high is used. The open-ended questions required narrative responses. The first part of the questionnaires was designed to gather institutional information while the remaining part was designed to gather information regarding actual implemented information security controls maturity level.

The questions help to assess and determine the maturity level of Information security as well the key factors that influence effective information security management in public Universities in Ethiopia. The data collection instrument was developed from a synthesis of literatures that are relevant to meet objective of this study. It was also based on the constructs in the research conceptual model. As it is also discussed under chapter 3, the design of the questionnaire questions items is mainly regarding of the ISO 27001:2013 information security management standard. Besides other related works which are presented and discussed under the previous literature review chapter are used. The questionnaires were first tested on the pilot study. The pilot study helps to check whether the survey instrument provided reliable and accurate information. The data collection is self-administered to respondents personally or via e-mail for some universities in the case where they are located spread geographically. Questionnaires were mailed and collected after completion.

4.4.2. Interview

Interview is a process in which the interviewer asks questions with the purpose of obtaining information and respondents answers (Murtala , 2015). A semi-structured interview outline (Appendix C) was designed and used for this study to gather a qualitative data. The interview helped to get the attitude and experiences from the target populations. The researcher selected the interviewees purposefully who are believed to be appropriate key informants about the subject matter. The target respondents were ICT directors and/or equivalent IT Security Manager Positions in the universities. It was conducted in person and via telephone in the case where the respondents located spread geographically. As the study attention is to assess the current maturity level of information security implementation in Ethiopian public universities, this interview instrument was selected to get the perspective of senior manager's position. It also helps to obtain detailed information and get deep information on what issues were going on in the Universities besides to the data collected using questionnaire. The Semi-structured interview contains a list of open-ended questions based on the topic areas.

4.4.3. Document Analysis

Document analysis was used to strengthen the analysis by referring different documents which includes: journal articles, books, conference papers, and documents prepared by the universities. The document analysis is used as a secondary data source to increase and support the data found with the other instruments which are the questionnaire survey and interview.

4.5. Pilot Study

A pilot study was conducted to test the feasibility of the study. The researcher selects one university for the pilot study and conducted the pilot study on IT professional staffs and checks the feasibility of the instruments. The pilot study assisted to ensure the instruments to be free inappropriate substances. Pilot study used to check the consistency of the questionnaire prior to distributing the survey at full-sized. The respondents were requested to evaluate the questions and using the relevant comments from the results of the pilot study some adjustments were made to make the content of the instruments more comprehensive for the study.

4.6. Data Collection Procedure

A list of specific questions was prepared by the researcher on important information security topics/areas regarding with industry best practices. The Designed questionnaires were administered to Participants personally and via email in some universities in the case where they are located spread geographically. The Participants were required to complete the questionnaires and email them back to the researcher. In addition, semi-structured interviews were administered to respondents to get more in-depth information. The Interview was conducted in person and via telephone in the case where the respondents located spread geographically.

4.7. Data Analysis

For the analysis process, the study generated both quantitative and qualitative data. Both types of collected data were analyzed in order to identify the relationships and patterns in the data.

Data analysis for quantitative studies, involves critical analysis and interpretation of figures and numbers, and attempts to find rationale behind the emergence of main findings. After the data is collected from the identified areas of data sources, firstly Data cleaning was conducted for possible omissions, missing items and errors and outliers. The Microsoft Excel software was used to analyze the quantitative data collected from the instrument.

Furthermore, In the research qualitative data analysis involve identifying common patterns within the responses and critically analyzing them in order to achieve research aims and objectives. The qualitative data is analyzed using open codding. It is presented in way providing explanations, understanding and interpretation of the phenomena, under the next chapter of the study.

CHAPTER FIVE: DATA PRESENTATION, ANALYSIS AND DISCUSSION

This chapter presents, analyzed and discussed the data obtained for the study regarding to the research objective. This study generated both quantitative and qualitative data. Both type of data was analyzed autonomously. This chapter has three main sections. The first part deals with the quantitative data presentation and analysis. The second part consists of the qualitative data analysis and discussion. Whereas, the third section of this chapter presents the discussion.

5.1. Quantitative Data Presentation and Analysis

Under this sub topic, the characteristics of the respondents, data relating to the institutes and the findings of the data is presented.

5.1.1. Respondent's Characteristics

5.1.1.1. Respondent's Job title and Responses Rate

This section deals with the analysis of the data collected from the sample population of respondents chosen from ten public universities. The instruments were administered to respondents personally or via email in some institutions. The study instrument is completed by the respondents presented in Table 6 below. 120 questionnaires were distributed to respondents identified as per sample size, 98 questionnaires were returned. This results the overall response rate to 81.6%.

Job title of Respondents	**Target**	**Received**	**Response rate in %**
Directors of ICT	10	7	70.0
Infrastructure, and Application development Division Head	20	15	75.0
Network Administrator	35	31	88.5
System Administrator	35	28	80.0
Application Developer	20	17	85.0
TOTAL	120	98	81.6

Table 6: Respondents Job title and percentage of responses

5.1.1.2. Respondent's Experience

The respondents were asked to indicate the number of years they worked in their university. As it can be seen from Table 7 below, the majority 48.0 percent of the respondents have working experience of three to five years. The 24.5 percent of the respondents have less than two years of experience. Whereas the 23.5 percent of the respondents have six to ten years of experience. The other 4.0 percent of the respondents eleven to fifteen years of experience working in the universities. This implies that the survey incorporated respondents with sufficient experience in the universities.

years of Experience	Frequency	Percent
2 years or less	24	24.5
3-5 years	47	48.0
6 - 10 years	23	23.5
11 - 15 years	4	4.0
Total	98	100.0

Table 7: Respondents' Experience

5.1.1.3. Respondent's Qualifications

The respondents were asked to indicate their qualification and the result is presented below in Table 8. shows the respondents qualifications. As it can be seen from the table 8, 93.9 % of respondents have a bachelor degree whereas the other 6.1% have a Master's degree. This indicates that, the survey incorporated respondents with adequate Qualifications.

Qualification	Frequency	Percent
Master's degree	6	6.1
Bachelor's degree	92	93.9
Total	98	100.0

Table 8: Respondents' Qualifications representation

5.1.2. Institutional Information

5.1.2.1. Information Security Management Standard

Below, Table 9 shows the respond regarding to whether the higher learning institutes have a standard or framework that they follow in the process of implementing Information security management system. As it can be seen from table 9, the majority 69.4 % of the respondents responded "No". The 22.4 % of the respondent's replay "Don't Know" whether their university have a standard or framework. Whereas the other 8.2 % of the respondent's replay "Yes".

Standard or framework	Frequency	Percent
Yes	8	8.2
No	68	69.4
Don't Know	22	22.4
Total	98	100.0

Table 9: ISM standard or framework in the institutes

5.1.2.2. Compromised with information Security Issues

The respondents were asked to indicate whether their institution has ever been compromised with information security issues in the last few years and the result is presented in table 10. It can be seen from the table 10, the majority 40.8 % of the respondent's replied "Yes". The 31.6 % of the respondents responded "No". On the other hand, 27.6% of the respondent's replied "Don't Know".

Compromised	Frequency	Percent
Yes	40	40.8
No	31	31.6
Don't Know	27	27.6
Total	98	100.0

Table 10: Compromised with information Security Issues

5.1.2.3. Information security personnel

Table 11 indicates whether the sampled institutes have personnel who are officially dedicated employed to handle IS security matters. It can be seen from the table 11, the majority 65.3 % of the respondent's replay "No". The 27.6 % of the respondents responded "Don't Know". Whereas, 27.6% of the respondent's replay "Yes".

Information security personnel	Frequency	Percent
Yes	7	7.1
No	64	65.3
Don't Know	27	27.6
Total	98	100.0

Table 11: Information security personnel

5.1.2.4. Existence of information security Policy

Respondents were asked in order to acquire whether their institution have Information security policy for ensuring security of information systems in their institute. As it is presented in table 15, it can be seen that the majority 48.0 % of the respondents indicated that their institute have information security policy which ensures security of information systems. Whereas 27.6 % of the respondents indicated that there was no Information security policy. On the other hand, 24.5 % the respondents "do not know" whether there is or there is no information security policy in their institute.

Standard or framework	**Frequency**	**Percent**
Yes	47	48.0
No	27	27.6
Don't Know	24	24.5
Total	98	100.0

Table 12: Existence of information security Policy

5.1.3. Maturity level Assessment

This sub chapter presented and analyzed the data collected for identifying the maturity level of the current information security implementation in Ethiopian public universities. The research framework which is discussed under chapter three of the study which is mainly regarding of identifying the maturity level of the current information security management practice in Ethiopian public university was analyzed using Microsoft Excel software. To represent the collected data Frequencies, Means, and percentages in a meaningful number were used to analyze the data. As it is discussed under chapter 3 part of the study, Information Security Practice Assessment areas were identified and presented along with the maturity assessment model. The assessment areas maturity level along with their result is presented on the next section. Also, the output of analyzing this section answered the research first and second question.

5.1.3.1. Maturity Level Results and Analysis

The application degree maturity of each control, domain or section were identified by classifying the response averages into five degrees based on what respondents granted with the 5-point level scale questionnaire, ranging from very low to very high. Accordingly, Responses' average (Mean) for each control, domain or ever section was calculated by Microsoft Excel software. As it is explained under chapter three which is the research framework section of the study, the SSE-CMM Capability Maturity Model (CMM) for System Security Engineering (SSE) model is used to give the score assessment on each area of the process that selected between 1 to 5 for each process area. Results of calculating the value of the maturity level is maturity index to obtain the level of maturity in accordance with Table 2 from chapter three.

The respondent's calculation result summary obtained per clause is shown in Table 13. Results of calculating the value of the maturity level (ranging from level 1-5) is maturity index to obtain the level of maturity in accordance with Table 3 from chapter 3. The results of the calculation to get the average value of the information security controls on Ethiopian higher education institutes regarding of the selected ten universities is 2.16 and the expected maturity level is 5 (Optimized). From this value we can conclude that the information security maturity level is on the second level i.e. repeatable but intuitive.

clause	Description	Index	Level
5	Information security policies	1.98	2
6	Organization of information security	1.99	2
7	Human resources security	1.90	2
8	Asset management	2.26	2
9	Access control	2.13	2
10	Cryptography	1.71	2
11	Physical and environmental security	2.22	2
12	Operational security	2.52	3
13	Communications security	2.36	2
14	System acquisition, development and maintenance	2.26	2
15	Supplier relationships	2.23	2
16	Information security incident management	2.36	2
17	Information security aspects of business continuity management	2.23	2
18	Compliance	2.04	2
Average		2.16	2

Table 13: Calculation of Maturity Level Result Summary of the universities

As it can be seen from the table above each annex A.5 to A.18 average is allocated to their equivalent score range in accordance with Maturity Level Assessment Criteria. The average of all Annex scores is below 2.5 and this make the annex to be at level 2. According to the maturity model, a result ranging from 1.51 to 2.50 is at level two which is 'Repeatable but Intuitive'. The average of these all annex is also results 2.16. The means regarding to the maturity Level range, it is level also on level 2. At this level 'Repeatable but Intuitive' referee to the institutions have a pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency. Furthermore, the detail maturity level result for each Higher Educational Institute can be seen in table 14.

As it can be seen from the above table12, the four uppermost maturities scored of Annex consequently are A.12 (Operational security) with a maturity score of 2.52, A.13 (Communications security) and A.16 (Information security incident management) with the same maturity score of 2.36, and Annex 14 (System acquisition, development and maintenance) with the same maturity score of 2.26. On the other hand, the bottom five Annex maturity level result consequently are A.10 (Cryptography) with a maturity score of 1.71, A.5 (Information security policies) with a maturity score of 1.98, A.6 (Organization of information security) with a maturity score of 1.99, A.7 (Human resources security) with a maturity score of 1.90 and A.18 (Compliance) with a maturity score of 2.04. Thus, these uppermost and lowermost maturity scored of the ISO 27001:2013 Annex in Ethiopian public universities is discussed in detail under the discussion section of the study.

The mapping of maturity level for all area in ISO 27001:2013 with the overall Maturity level result per Annex is presented in a graphic way in figure 13. As it be seen from figure 13, all the average of all Annex scores revolves around in between 1.71- 2.5 and gives the overall average of these all annex to be 2.16 (level 2).

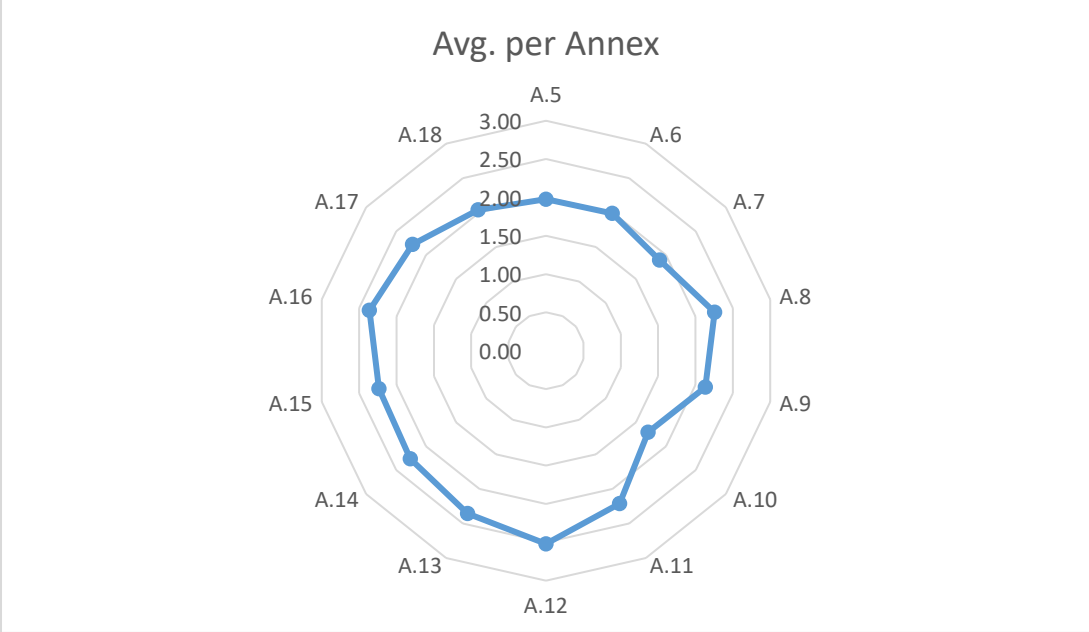

Figure 10: Maturity level result per Annex

Maturity level per the Higher Education Institutes (HEI)

The maturity level for each selected ten higher education institutes is presented below in figure 14. The 1st Generation universities (HEI 01, HEI 02 and HEI 3) scored an average score of 2.25 approximately. The Second-generation universities (HEI 04, HEI 05, HEI 06 and HEI 07) scored an average score of 2.17 approximately. Whereas the third-generation universities (HEI 01, HEI 02 and HEI 3) scored an average score of 2.04. Thus, discussed relating to the higher education institutes is presented in detail under the discussion section of the study.

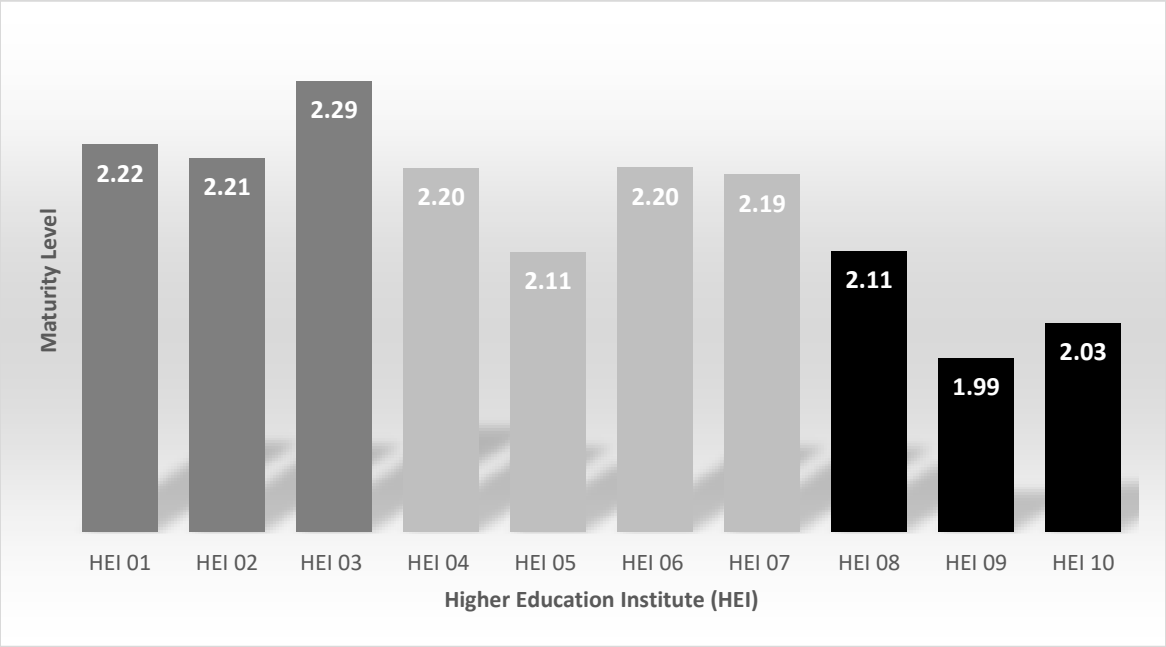

Figure 11: Maturity level result per Higher Educational Institute

Higher Education Institute (HEI)	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
HEI 01	2.13	1.91	2.05	2.27	2.12	1.78	2.23	3.03	2.32	2.24	2.14	2.41	2.32	2.21
HEI 02	2.05	2.04	1.85	2.05	2.37	1.50	2.25	2.46	2.40	2.60	2.45	2.45	2.30	2.17
HEI 03	2.19	2.25	1.85	2.30	2.27	1.71	2.35	2.53	2.60	2.43	2.30	2.60	2.50	2.23
HEI 04	1.96	1.85	2.1	2.35	2.30	1.86	2.3	2.73	2.35	2.26	2.25	2.40	2.20	1.87
HEI 05	1.90	1.95	1.95	2.25	2.03	1.71	1.95	2.43	2.30	2.20	2.25	2.30	2.30	1.97
HEI 06	1.87	2.17	1.94	2.33	2.30	1.57	2.39	2.30	2.50	2.33	2.11	2.44	2.39	2.15
HEI 07	2.08	1.95	2.18	2.27	2.18	1.88	2.27	2.48	2.41	2.30	2.27	2.32	2.14	1.94
HEI 08	2.11	2.00	1.93	2.15	1.90	1.71	2.35	2.37	1.95	2.37	2.35	2.40	2.05	1.87
HEI 09	1.63	1.94	1.44	2.25	1.88	1.67	2.13	2.33	2.38	1.85	2.06	2.19	2.06	2.08
HEI 10	1.85	1.83	1.67	2.33	2.00	1.67	1.94	2.52	2.39	2.04	2.17	2.11	2.00	1.89
Avg. per Annex	1.98	1.99	1.90	2.26	2.13	1.71	2.22	2.52	2.36	2.26	2.23	2.36	2.23	2.04

Table 14: Detail maturity level result for each Higher Educational Institute

5.1.3.2. Maturity Level Gap Analysis

Knowing the maturity level of information security is currently at 2.21 (Repeatable but intuitive) and the expected maturity level is 5 (Optimized). First by getting the value gap for each clause and then all values are summed gap then averaged to obtain the value of the overall gap. The value of the gap between current security conditions and the condition of the expected is 2.84. The Maturity Level gap can be seen in table 14.

Clause	Description	Maturity Level		Gap
		Current	Expected	
5	Information security policies	1.98	5.00	3.02
6	Organization of information security	1.99	5.00	3.01
7	Human resources security	1.90	5.00	3.10
8	Asset management	2.26	5.00	2.74
9	Access control	2.13	5.00	2.87
10	Cryptography	1.71	5.00	3.29
11	Physical and environmental security	2.22	5.00	2.78
12	Operational security	2.52	5.00	2.48
13	Communications security	2.36	5.00	2.64
14	System acquisition, development and maintenance	2.26	5.00	2.74
15	Supplier relationships	2.23	5.00	2.77
16	Information security incident management	2.36	5.00	2.64
17	Information security aspects of business continuity management	2.23	5.00	2.77
18	Compliance	2.04	5.00	2.96
Average				2.84

Table 15: Maturity Level Gap Calculation

Legitimately there is a large gap, value proportion to the current maturity level and the value of the expected maturity level are discussed as follow. In addition, Recommendations is also given regarding on the improvement the required adjustment of weak controls.

5.2. Qualitative Data Analysis

Besides to the quantitative study presented in pervious section of this chapter, qualitative data was collected to enhance the findings of the study. In this section, the analysis of this qualitative data of the study which is done throw Interview is presented. The interview helped to get the attitude and experiences from the target populations which are directly related to the subject matter. The target respondents were ICT directors in the universities. This provided input from the perspective of a senior manager's position in the subject matter. Accordingly, interviews have been conducted with Three ICT directors form the three different generation categorized universities. For the purpose of confidential and ethics of research the interview are renamed as interviewee 01, interviewee 02 and interviewee 03 throw out the analysis process. The output of analyzing this section should answer the third research question of the study and also supports the other two research question answers. The information gathered from the interviews was described in terms of words. The interviewees were interviewed regarding of two categories. First, the description of the current status and key issues of information security implementation. And, the identification of suggested strategies for possibly improvements in information security management is proposed.

The interviewees were requested to describe their current approaches that are taken to manage Information and information systems Security in addition to explain the drawbacks and strengths of the existing approaches for managing Information Security. All the interviewees replied that there is no stated function for managing information and information security matters and there is a lack or a gap of knowledge for the management of Information Security. It is indicated that their institutions lacked a dedicated security function. They admit that the absence of a dedicated security professional and controls impacted the institution's ability. In most cases, information security related tasks are handled by other professional such as system and network administrators. In this regard one of the interviewee 01 replied that "There are no dedicated personnel who are responsible for information systems security matter, but such kind of tasks handled by system and network administrators along with their defined tasks". The results obtained through interview are in line with the questionnaire findings. From this interviewee result, it can be notice that institutes clearly lack experienced personnel who are officially dedicated to handle IS security matters.

In addition, two of the interviewee mentions that there is no formal developed ISMS framework or standard that the institution follows in the process of implementing Information systems security. Also, it is pointed out that there are non-formalized policies and procedures which are approved by top management to be used to control and protect the information asset. It is also indicated that, currently an official information security policy document is being drafted and will be used in the future. Interviewee 03 replied that "Security Devices like Proxy Firewall both Hard ware and Software between the trusted and un-trusted network is used. Even if we use those security devices but we don't have clear security policy and no dedicated professional that control the activities like log files". This shows that there is an absence of formal ISMS framework or standard used to be handled security issues. This result obtained through interview also in line with the questionnaire findings.

The interviewees were requested on how possible improvement regarding of information security management be achieved in the future. Based on their experience, the interviewees put their perspective and future possible improving ideas. Interviewee 02 suggested that "The formulation of information security management and a security policy is necessary and mandatory because their nothing to follow in the process of implementing Information systems security". Here also the results obtained through interview are identical to the questionnaire findings. This shows that a structured and coordinated approach was needed to improve effectiveness of current information security management approaches. Meaning by the Developing and use for standard is a more structured and coordinated management framework for progressing security within the university community is an essential step in delivering improved security management. In addition, a formulation of information security policy and an information security management framework are issues that are needed to be addressed.

The other point raised by the interviewees is regarding creating IS awareness for the employees. Interviewee 03recommended that "first of all a for the ICT staffs with little concept and awareness of information and information system security need to be educated on security matters. At a regular base training on how information systems security need to be prepared and given to the staffs". In addition to this Interviewee also supports this idea and said that "Besides of creating comprehensive Information security policies (ISP), culture of compliance towards

security need to be notices strategic goal to aim for, involving increased awareness of security issues. Moreover, the finding is also supports the result from the questioner survey results. In Several scholars stated that good security awareness program should include communications and periodic reminders to employees (Bilal , Khaled , Syed , & Muhammad , 2011). Thus, training on the security best practice and issues will improve employee's overall knowledge and understanding of potential issues related to information security and their difficulties.

5.3. Discussion

- **First research question:**

"What is the current maturity level of information security implementation in Ethiopian public universities sector?"

The measurement of the maturity levels indicates the relevant security processes that the institutes implemented to achieve the security of information and information security systems. The value of the maturity level (ranging from level 1-5) is maturity index to obtain the level of maturity in accordance with the Maturity Level Assessment Criteria. The measurement of maturity level of information security which is calculated regarding of the System Security Engineering Capability Maturity Model (SSE CMM) as it also discussed in pervious chapters.

The results of the calculation of the questionnaire managed to get the average value of the information security controls on Ethiopian higher education institutes regarding of the selected universities is 2.16 and the expected maturity level is 5 (Optimized). From this value it is conclude that the information security maturity level is on the second level i.e. repeatable but intuitive. The value of the gap between current security conditions and the condition of the expected is 2.84. Legitimately there is a large gap, value proportion to the current maturity level and the value of the expected maturity level. Thus, the results Level 2 Information Security efforts are at a repeatable level where basic project management techniques are established and successes can be repeated. Though pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency.

As it is discussed under chapter four, the nature of the universities existence is in generation-based strata. Meaning by the universities are already created a stratum based on their establishment time and the moment of upgrade from college to university. like wisely, the universities were clustered in to three generations. Also, the study assumes that the pioneer universities established in the sector, the more stable and experienced on the subject matter. Consequently, the average of the overall maturity level which is resulted 2.16 can be also be seen distinctly by looking into the higher education institutes. It can be seen in figure 14 from the previous section, the 1st Generation universities (HEI 01, HEI 02 and HEI 3) scored better maturity score relatively comparing to other Higher Education Institutes as they are existed earlier in the business or so called "1st Generation universities" with an average score of 2.25 approximately. Relatively, the Second-generation universities (HEI 04, HEI 05, HEI 06 and HEI 07) scored an average score of 2.17 approximately. Whereas the third-generation universities (HEI 01, HEI 02 and HEI 3) scored an average score of 2.04. These results show that that the pioneer universities established in the sector, the better score and experienced on the subject matter.

- **Second research question:**

"What are the uppermost and lowermost maturity scored information security controls in Ethiopian public universities?"

Besides to identifying the maturity level of information security in the Ethiopian higher learning institute, this study had also a purpose to identify the uppermost and lowermost maturity scored information security controls implement. These uppermost and lowermost maturity scored information security controls are discussed below.

Uppermost maturity level scored information security controls

As it is also mentioned in the previous section, the top four maturities Annex level were A.12 (Operational security) with a maturity score of 2.52, A.13 (Communications security) and A.16 (Information security incident management) with the same maturity score of 2.36, and Annex 14 (System acquisition, development and maintenance) with the same maturity score of 2.26. Annex 12 is about Operational security and scored 2.52 maturity levels. It's the highest score and also the smallest maturity gap 2.48 from the entire annexes. Under this control management of IT

production including malware, backup, logging and monitoring is taken place. Institutions have given attention of taking back up of essential information and also Processes to detect malware to prevent malware spreading are place even though it is not effective on the expected optimized level.

The second highest scores are Annex 13 and Annex 16 with the same maturity score of 2.36. Annex 13 is about Communications security and Annex 16 is for Information security incident management. In the communication security process, Network management process are taken place to prevent non-authorized forms of data transfer and traffic originating from un-trusted network in to the institutes are flittered by firewall. Though it is at the intuitive level the annex Information security incident management is considered and assisted the institutes to ensure information security events and weaknesses associated with information systems to be communicated in a manner but there is a defective timely respond for corrective action to take. The third highest score is 2.26 which is for Annex 14 and it is about the System acquisition, development and maintenance. According to the respondents all institutes develop software or systems that are used in conducting their occupational process but this software development projects does not utilize the proper secure development environment appropriately during the system development lifecycle.

lowermost maturity level scored information security controls

The bottom Five Annex maturity level result consequently are A.10 (Cryptography) with a maturity score of 1.71, A.5 (Information security policies) with a maturity score of 1.98, A.6 (Organization of information security) with a maturity score of 1.99, A.7 (Human resources security) with a maturity score of 1.90 and A.18 (Compliance) with a maturity score of 2.04. Annex 10 is about Cryptography with a maturity level result of 1.71. This is the least maturity level from the entire annex's, in which it has also the highest maturity gap of 3.29. This control is related to encryption and key management. The institutes implemented encryption through the use of firewall but the whole lifecycle of cryptographic process is not governed using the appropriate regulation. On the other hand, the second lowest maturity score is Annex 5 which is regarding of Information security policies. As this control is on how the policies are written and reviewed Security policy, it is important to provide management direction and support for information

security in accordance with business requirements and relevant laws and regulations. Most respondents indicate that institutes do not have a properly recognized information security policy that is official acknowledged by top management.

The other Annex with the lowest score of 1.99 is Annex 6 and it is about the organization of information security. Organization of Information Security is about of the establishing a management basis to initiate and control the implementation and operation of information security and responsibilities for the protection of informatics assets out within the organization. According to the result institutes do not clearly defined responsibilities for the protection of individual informatics assets and for carrying out specific security processes. Also, the institutes do not have personnel who are officially dedicated employed to handle IS security matters. These tasks are done with other professionals namely system and network administrators as an additional task. This leads to miss out the day-to-day management of IT Security in institutes because of there is no official personnel who is specialized and in charge regarding of in the security issues.

The Annex 7 has also a low score of 1.90. Annex 7 is about Human resources security. This controls deals with the prior to employment, during, and after the employment human resource security. Security issues should be addressed during the recruitment stage, in contracts and during an individual's employment. Majority of the respondents indicated that security roles and responsibilities are not included in terms and conditions of employment in their university. To ensure that employees, contractors and third-party employees must understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. The other annex with weakest maturity level score is A.18. The Annex 18 is about Compliance and has got a maturity level of 2.04. This control ensures the compliance of systems with organizational security policies and standards and to maximize the effectiveness. But, As the maturity level shows and respondents indicate the culture of compliance towards information security is not reflected through institution's work practices.

- **Third research question:**

"How could potential improvements in information security be achieved in Ethiopian public universities??

As the result shown in the previous section, the current implementation of Information security maturity level in Ethiopian public universities is not optimized. In order to improve the information security management some indications are put from the qualitative data. Considering the presented result of the qualitative data, in which interviewees requested on how possible improvement regarding of information security management be achieved in the future the following paragraphs summarize the areas has to be considered for future improvement in the sector.

The adoption or the formulation of information security management framework or standard is one area that need consideration. This includes the establishment of major security controls that are necessary in protecting information and information systems exit in the institutes. As per the result of the study, majority of the respondent indicate that their institutes do not have a standard or framework that they follow in the process of implementing Information security management system. A systematic information security approach is necessary for the arrangement or structuring of information security components to implement information security in an effective manner.

The formulation and use of Information security policy is another area that needs attention and improvements. As it presented in the previous section, the majority of the respondents indicated that their institute do not have information security policy and even "do not know" whether there is or there is no information security policy in their institute. This shows the lack of making employees to be aware of the existence as well the culture of conducting their work in according to the rules and increases the culture of compliance with the regulations accordingly. Consequently, universities have to formulate Information security policy regarding of the best security practices and information systems exist in their institute. In line with this, scholars have empirically emphasized that information security policy is an official document of the organization strategy in the security area and contains explicit measures and procedures as well the behavioral framework (Pavlov & Karakaneva , 2011).

CHAPTER SIX: CONCLUSION, RECOMMENDATIONS AND FUTURE WORKS

This chapter provides a conclusion by summarizing the research outcomes, providing recommendations drawn from the study and suggestions for future study.

6.1. Conclusion

The intention of this study was to investigate the to assess the current maturity level of information security management practice in Ethiopian public universities and analyze the maturity result to give recommendations for future improvements.

Based on Systems Security Engineering Capability Maturity Model (SSE-CMM) which is a straight forward analysis of existing processes to determine which base processes have been met and the maturity levels they have achieved; the result of security were analysis regarding of the questionnaire managed to obtain an average value for all of the clauses of ISO 27001 was 2.16. As Result of calculating the value of the maturity level (ranging from level 1-5) which is maturity index to obtain the level of maturity from this value as it is discussed in the previous chapter in accordance with SSE-CMM, we can conclude that the security of information is level 2 (repeatable but intuitive) range from level 0 (none) to level 5 (optimistic).

Level 2 (repeatable but intuitive) referee to the institutions have a pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency. The average of the overall maturity level which is resulted 2.16 also seen separately by looking into the higher education institutes. the 1st Generation universities scored better maturity score relatively comparing to other two Higher Education Institutes generation, as they are existed earlier in the business Whereas the third-generation universities found to be at the bottom. These results show that that the pioneer universities established in the sector, the better score and experienced on the implementation of information security.

This study also pursued to investigate the lowermost maturity level scored security control areas in which Cryptography, Information security policies, Organization of information security, Human resources security, and Compliance found to be very weak. However, these security controls areas need improvements. By Organizing a better of Information Security control plus personnel who are officially dedicated employed to handle IS security matters besides to establishing a management basis for controlling the implementation as well operation of information security and responsibilities for the protection of informatics assets can be ensured.

6.2. Recommendations

Based on the findings obtained from the analysis of the study, recommendations for improvement of the current condition are presented on the following paragraphs.

Institutions without information security policy have to formulate one by include specified procedures in the security matters. policies and procedures have not been documented in some institutes, even security related works are conducted by impulsiveness and without any regular form. Access control rules and rights for each user or group of users should be clearly stated in a policy statement. The access rights of each employee's and updating of access rights in case of transfer or advancement must made in accordance. Information security emphasized that management's attention is required to secure information resources to design effective security policies, and to enhance users' security awareness of information security policies. People are recognized as the weakest link in the information security chain but are considered abundant assets in the effort to reduce information security threats Therefore, security policies and procedures should be formulated, documented, have to be available for employee's and maintained accordingly. Improving information security policy controls can provide direction and support to the ISMS by the implementation, communication, and controlled review of information security policies.

Human resource security is also another security control that need improvement. Human resource security issues should be addressed during the recruitment stage, in contracts and during an individual's employment. Rules about information security responsibilities in the employment contract should also be included. Every employee, contractor or third party should return all the

institutions assets used for work depending on the contract, when the employee, contractor or third party leave the institute. Improving Human resource security will help the institutes to ensure that employees fit for working and know their responsibilities, and that any changes in employment conditions will not affect information security.

Based on the finding of this study the Organization of information security control in the Higher Education Institutes is weak. The information systems should be controlled and physically well protected to prevent damage to assets and interruption to institutes activities. Appropriate procedure should be established to protect documents, computer systems, the data input / output and documented system from damage, theft and unauthorized access. The improvement and well implementation of the Organization of information security controls provide the basic framework for the implementation and operation of information security by defining its internal organization in the Higher Education Institutes.

The other information security control area that need improvement is Cryptography. The controls in this section aim to provide the basis for proper use of cryptographic solutions to protect the confidentiality, authenticity, and/or integrity of information. Even though, Institutes implemented encryption through the use of security devices but governing using the appropriate regulation also essential.

Higher Education Institutes have to give trainings on information security controls and regulation in order to increasing the culture of compliance. Compliance with organizational security policies and standards maximize the success information security management. Compliance 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, and procedures. To maintain compliance with information security policies, managers have to make decisions on the use of effective techniques to deal with non-compliance; these include correctional responses like sanctions, information security training or additional systems security features and layers.

6.3. Future Works

As the research aimed to assess the current maturity level of information security management practice in Ethiopian public universities and analyze the maturity result to give recommendations for future improvements. This study can be used as a preliminary for further researches. For further future works, the following are the researcher's suggestions:

- Construction of an Information security management framework for the Ethiopian higher education sector.
- Formulating a standard information security policy in Ethiopia's Higher Learning Education sector.
- To investigate on factors that hinders the effectiveness of information security management.

REFERENCES

Ahmad , A., Amit , D., Omar , E., Jack , W., & Hasan , A. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *46th Hawaii International Conference on System Sciences.* IEEE .

Ateeq , A. (2012). Type of Security Threats and It's Prevention. *International Journal Computer Technology & Applications, Vol 3 (2).*

Azah , N., & Norizan , Y. (2010). A Critical Review of Information Systems Security Management (ISSM) Implementation: Comparison between Stable Organizations and Emergent Organizations. *International Journal of Digital Society (IJDS), Volume 1, Issue 3*.

Bertrand , M. (2012). *Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees.*

Bhawna , & Gobind . (2015). Research Methodology and Approaches. *Research Methodology and Approaches*, 48-51.

Bichanga , W., & Obara , B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa – Kenya. *International Journal of Management Excellence Volume 3 No.1* .

Bilal , K., Khaled , S., Syed , I., & Muhammad , K. (2011). Effectiveness of Information Security Awareness Methods Based on Psychological Theories. *African Journal of Business Management Vol. 5(26),* 10862-10868.

BSI- standard 100. (2008). *BSI- standard 100 Information Security Management System(ISMS). Bundesamt für Sicherheit in der Informationstechnik (BSI).* Godesberger Allee.

Burcu , B., Hasan , C., & Izak , B. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly Vol. 34 No. 3,* 523-548.

Candiwan, Puspita , K., & Nadiihaq , N. (2016). Assessment of Information Security Management on Indonesian Higher Education Institutions. *Springer Book Lecture Notes in Electrical Engineering Series, Vol. 362,* 375-385.

Carrie , W. (2007). Research Methods. *Journal of Business & Economic Research, Volume 5, Number 3*.

Christophe , V. (2016). *Maturity Assessment, Profile, and Plan A MAPP to Clearer Information Security.* Secure digital solution.

Daniel, M., & Peter, W. (1999). Measuring The Value Of Information:. *European Conference on Information Systems (ECIS'99)*, (pp. 1-17). Denmark.

Deborah , S., Pamela , R., Linda , C., & Ronald , F. (2004). Evaluation of The Human Impact of Password Authentication Practices on Information Security. *Informing Science Journal,Volume 7*.

EFDR MOE. (2010). From the Education world. *21th Annual Education Training conference. Volume 1, number 2.* Addis Ababa.

Endang , K., & Imam , R. (2018). Security Level Analysis of Academic Information Systems Based on Standard ISO 27002: 2013 Using SSE-CMM. *International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 1*.

Fulford , H., & Doherty , N. (2003). The Application of Information Security Policies in Large UK based Organizations: An exploratory investigation. *Information management and computer security, Vol. 11, No. 3.*

Georg, D. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 92-100.

Gigi , D. (2017). What Is a Stratified Random Sample? Match Sample Type to Research Purpose.

Hong , C., & Sameera , M. (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications, Volume 60– No.10*.

Ilker , E., Sulaiman , A., & Rukayya , S. (2015). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics. Vol. 5, No. 1*, 1-4.

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

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

Jack, G. (2002). *The Basics of an IT Security Policy: GSEC practical Requirement V.1.3.* Global Information Assurance Certification (GIAC).

Kelemie , T. (2013). *Information Security Management Framework for Banking Industry in Ethiopia.* Addis Ababa: Addis Ababa University.

Knut , H., Ricardo , C., Srdan , D., Knud , B., & Vladimir , S. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management, Vol. 4, No. 4*, 27-47.

Ladan, S., Yari, A., & Khodabandeh, H. (2006). Combination of Information Security Standards to Cover National Requirements. *World Academy of Science and Technology.*

Lenka, F., & Roland , M. (2012). *Threats, Risks and the Derived Information Security Strategy.* Springer Fachmedien .

Lloyd , M. (2012). *An Appraisal of Information Security Management at Chancellor College, University of Malawi.* Luleå University of Technology.

Mark , R. (2013). *information Security: The Complete Reference 2nd edition,.* USA: McGraw.

Mehdi , K., Hamid , K., & Hashem , N. (2012). Evaluation of Information Security Management System Success Factors: Case Study of Municipal Organization. *African Journal of Business Management Vol. 6(14),* 4982-4989.

Mouna , J., Latifa , B., & Anis , B. (2014). Classification of security threats in information systems. *5th International Conference on Ambient Systems, Networks and Technologies* (pp. 489 – 496). Procedia Computer Science .

Murtala , G. (2015). A Critical Analysis of the Techniques for Data Gathering in Legal Research. *Journal of Social Sciences and Humanities Vol. 1, No. 3*, 266-274.

Mwita , S. (2015). *Factors Affecting Information Systems Security Effectiveness in University of Nairobi.* Nairobi: University of Nairobi .

NIST. (2012). *Computer Security Incident Handling Guide. Special Publication 800-61 Revision 2.* National Institute of Standards and Technology .

NIST SP. (1998). Generally Accepted Principles and Practices for Securing Information Technology Systems.

Noli , B. (2016). Information Security Policy Development: A Literature Review. *International Journal of Innovative Research in Information Security (IJIRIS),Volume 3* .

Pavlov, G., & Karakaneva , J. (2011). Information Security Management System in Organization. *Trakia Journal of Sciences, Vol. 9, No 4*, 20-25.

PCI. (2016). Requirements and Security Assessment Procedures Version 3.2.

Philip , M. (2013). *Information Security Management Systems in Public Universities in Kenya: A Gap Analysis Between Common Practices and Industry Best Practices.* University of Nairobi .

Puspita , K., Nadiailhaq , N., & Candiwan . (2013). *Factor Analysis on Information Security Management in Higher Education Institutions.* Indonesia : University Bandung.

Qingxiong , M., & Pauline , R. (2008). Factors Affecting the Objectives of Information Security Management. *CONFIRM* .

Rasha , A., & Marini , O. (2013). COBIT Framework as A Guideline of Effective It Governance in Higher Education: A Review. *International Journal of Information Technology Convergence and Services (IJITCS) Vol.3, No.1*.

Razieh , S., & Nasser , M. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology Vol. 5 No. 2*.

Rosmiati, I., & Yudi , P. (2016). A Maturity Level Framework for Measurement of Information Security Performance. *International Journal of Computer Applications, Volume 141 – No.8.*

Salahuddin , M. (2011). *Information security management: A case study of an Information security culture.* Queensland university of technology .

Sattarova , Y., & Tao, K. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *international Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, .*

sector, I. e. (n.d.). researcher's experience and communication with IT experts in education sector.

Simon , K. (2014). Information Security Management for Higher Education Institutions. *Intelligent Data Analysis and Its Applications, Volume 1*.

Sitwala , I. (2014). IS There a Conceptual Difference between Theoretical and Conceptual Frameworks? *Journal of Social Science*, 185-195 .

Solms, R. (1998). Information security management: the code of practice for information security management. *Information Management Computer Security*, 224-225.

SSE-CMM. (1991). *System Security Engineering Capability Maturity Model (SSE-CMM) Description Document Version 2.0.* System Security Engineering Capability Maturity Model (SSE-CMM) project.

Tim , L. (2007). *Information security management in Australian universities: An Exploratory Analysis.* . QUT Faculty of Information Technology School of Software Engineering and Data Communications .

Wilco, E. (2007). Information Assets and their Value. *6th Twente Student Conference on IT*.

Wolfgang , H., Stefan , M., & Michael , S. (2012). *Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization.* Munich: Leibniz Supercomputing Centre.

APPENDICES

Appendix A: Letter of Request

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date April 2, 2018
Ref: -SIS/17 /2018

To Whom It May Concern

Student **Nebyu Ejerssa** (ID.No. GSE/0393/08) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "Assessment of Information Security Management on Ethiopian Public Universities".

I would like to thank you in advance for all the assistance that you would provide to the student.

With Regards,

Martha Yifiru (PhD)
Head, School of Information Science

✉: 1176 ☎: +251-(11)-122-91-91 ☎:2122- 91-92

Appendix B: Questionnaire Survey

Introductory letter

Dear Sir/Madam,

My name is Nebyu Ejerssa and I am undertaking a research entitled "Assessment of Information security management on Ethiopian public universities "In partial fulfillment of the requirements for the Degree of Master of Science in Information Science at Addis Ababa University. I am inviting you to participate in this research study by completing the attached questionnaire.

The research aims to investigates the current information security management practices in public universities in Ethiopia. It attempts to determine and analyze the gap in contributing the successful implementation and future progress of information security in public Higher Learning Institutions in Ethiopia.

The following questionnaire will require approximately 20 to 25 minutes to complete. Any information provided will be treated in the strictest confidence. You may also wish to consult with colleagues in your institution about answers to particular questions. Any enquiries you may have concerning this research study could be directed to me by the address mentioned below.

I appreciate your time and honesty contribution in responding the questionnaire. Thank you very much for your cooperation.

Sincerely

Nebyu Ejerssa.

Email:

Phone:

Information Security Management Questionnaire

Part I: General Information

Survey ID: ……

Name of the University: ……

Please put x letter in the box that related to your answer.

1. Respondent's Information

1.1.Respondent Job Title ……

1.2.Qualification:

[ ]PhD [ ]Master's degree [ ] Bachelor's degree [ ]Diploma [ ]TVET Level

1.3.years of Experience:

[ ]2 years or less [ ] 3- 5 years [ ] 6 - 10 years [ ] 11 - 15 years [ ] More than 15years

2. Organizational Information

2.1.How many branch campuses does your institution have?.....

2.2.How many staff does your institution employ?.....

2.3.How many students your institution has? .....

2.4.How many IT staff does your institution have? ……

2.5.Has your institution ever been compromised with information security issues in the last few years? [ ] Yes [ ] No [ ] Don't Know

- If yes, was the institution compromised internally, externally or both?

[ ]Internally [ ] Externally [ ] Both

2.6.Is there a standard or framework your organization follow in the process of implementing Information systems security? [ ]Yes [ ] No [ ] Don't Know

- Incase yes please choose:

[ ]ISO [ ] PCI [ ] COBIT [ ] ITIL [ ] other please specify …….

2.7.Does the University have personnel who are officially dedicated employed to handle IS security matters? [ ] Yes [ ] No [ ] Don't Know

- In case "No" How is the Information security related tasks are handled in the institution?

……

Part II: Current State of Information Security Management.

Please put x letter in the box that related to your answer.

	Organization of information security
1.	Responsibilities for the protection of individual informatics assets and for carrying out specific security processes were clearly defined. [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
2.	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls. [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
	Human resources security
3.	Are security roles and responsibilities clearly stated in your institution's terms and conditions of employment? [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
4.	background verification checks carried out on all new candidates for employment and approved by management authority? [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
	Asset management
5.	All assets associated with information and information processing facilities are clearly identified, classification and inventory take place regularly? [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
6.	There is process to ensure employees and external users return the organization's information assets on termination of their employment, changing duties, contract and remove access right in an appropriately? [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
	Information Security policy
*	Does your institution have an information security policy? [ ] Yes [ ] No [ ] Don't Know
7.	If you answered "yes" in Question 1, Are information security policies properly published, available, communicated to all employees? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
8.	The information security policy considers all stakeholders such as employees, contractors, venders, service providers, and students? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
9.	Are security policies subject to review and conducted when circumstances change? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high

10.	The security policy is fully implemented and It is highly effective in ensuring IS security. [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
*	If you answered "No" in Question 1, please explain the means through which information systems security regulations is maintained in the institute.?
	Access control
11.	Access controls are in place to ensure users only have access to the restricted resources (secure areas) they have been specially authorized to use? [ ]1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high
12.	Is there a user access control policy document for granting access to users of information systems and services? [ ] Yes [ ] No [ ] Don't Know
13.	There is a process in place that ensures users follow good security practices in the selection and use of passwords? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate[ ] 4.High [ ] 5.Very high
14.	An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
*	Please State what type of physical controls are implemented and where?
	Cryptography
15.	Has your institution implemented encryption? [ ] Yes [ ] No [ ] Don't Know
*	In case "Yes" The whole lifecycle of cryptographic process is governed using appropriate regulation. [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	Physical and environmental security
16.	Power, telecommunication cables and wireless communication carrying data or supporting information services are protected from interception or damage. [ ] 1.Very low[ ] 2.Low [ ] 3.Moderate[ ] 4.High [ ] 5.Very high
17.	Secure areas are physical protected against damage from fire, flood, earthquake, explosion, student unrest, and other forms of natural or man-made disaster been designed in? [ ] 1.Very low[ ] 2.Low [ ] 3.Moderate[ ] 4.High [ ] 5.Very high
	Operational security
18.	Processes to detect malware and prevent malware spreading in place and regularly updated? [ ] 1.Very low[ ] 2.Low[ ] 3.Moderate[ ] 4.High [ ] 5.Very high

19.	Back up of essential information taken regularly? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
20.	A process takes place to control the installation of software on to operational systems? [ ] 1.Very low [ ] 2.Low[ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	Communications security
21.	Network management process in take place to prevent non-authorized forms of data transfer? [ ] 1.Very low [ ] 2.Low[ ] 3.Moderate [ ] 4.High [ ] 5.Very high
22.	Is all the traffic originating from un-trusted network in to the organization flittered by firewall and web security for malicious? [ ]1.Very low [ ] 2.Low[ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	System Acquisition, development and maintenance
23.	Are information security requirements specified and addressed when new systems are introduced, enhanced or upgraded? [ ] 1.Very low [ ] 2.Low[ ] 3.Moderate [ ] 4.High [ ] 5.Very high
24.	Does your institute develop software or systems? [ ] Yes [ ] No [ ] Don't Know
*	Incase "yes", do all projects utilize the secure development environment appropriately during the system development lifecycle? [ ] 1.Very low[ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
25.	Do applications which send information over public networks appropriately protect the information against fraudulent activity, contract dispute, unauthorized discloser and unauthorized modification risk? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	Supplier Relationships
26.	Information security is always included in contracts established with suppliers and service providers? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
27.	Is supplier access to information assets &infrastructure controlled and monitored? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	Compliance
28.	There is a clear procedure to discipline members who violate organizational security policy and regulations. [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high

29.	Does the organization regularly conduct technical compliance reviews and instruct managers to regularly review compliance with policy and procedures within their area of responsibility? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
30.	Is the culture of compliance towards information security reflected through your institution's work practices and business processes? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	Information security incident management
31.	Is there an incident response plan and process which reflects the classification and severity of information security incidents? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
32.	Is there a process for timely reporting of information security events and weaknesses as well acting on reported information security events? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
	Information security aspects of Business continuity management
33.	Information security is included in the organization's business continuity plans? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high
34.	Does the organization's information security function have documented, implemented and maintained processes to maintain continuity of service during an adverse situation? [ ] 1.Very low [ ] 2.Low [ ] 3.Moderate [ ] 4.High [ ] 5.Very high

Thank you for your Time!

Appendix C: Interview Outline

Information Security Management Interview Questionnaire

1. Please, describe your institution's current approaches that are taken to manage Information and information systems Security?
2. What are the drawbacks and strengths of the existing approaches for managing Information Security?
3. Please, List and describe, what are to be the key issues influencing the successful implementation of information security management system in your institute?
4. In your view, please Describe What type of things need to happen or done to improved and achieving effective information security in your institution?

Appendix D: Detail List of Accredited list of Public Universities in Ethiopia

No.	University	Generation	Period of time	Status	Remark
1	Addis Ababa University	1st Generation universities	1996-1999	Existed	2pioneer universities are existed
2	Haramaya University			Existed	
3	Hawassa (Debub) University		2000-2004	Upgraded	During this period 5 colleges are upgraded to university level and only Mekelle university newly opened
4	Jimma University			Upgraded	
5	Gonder University			Upgraded	
6	Bahir Dar University			Upgraded	
7	Arba Minch University			Upgraded	
8	Mekelle University			New	
9	Dilla University	2st Generation universities	2004-2008	Upgraded	During this period Dilla and Adama universities are upgraded to university level from college level and 11 new universities are opened.
10	Adama University			Upgraded	
11	MizanTepi University			New	
12	MadaWalabu University			New	
13	Semera University			New	
14	Debre Markos University			New	
15	Wollo University			New	
16	DebreBirhan University			New	
17	Aksum University			New	
18	WolaitaSodo University			New	
19	Dire Dawa University			New	
20	Wollega University			New	
21	Jijiga University			New	
22	Ambo University	3st Generation universities	2009-2014	Upgraded	During this period Ambo university is upgraded to university level and 9 new universities are opened.
23	Metu University			New	
24	Bule Hora University			New	
25	Addis Ababa Science and Technology University			New	
26	Debre Tabor University			New	
27	Woldiya University			New	
28	Asosa University			New	
29	Adigrat University			New	
30	Wachamo University			New	
31	Wolkite University			New	

Source: Federal Democratic Republic of Ethiopia Ministry of Higher Education (2010)