ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

FORMULATING AN INFORMATION SECURITY POLICY FRAMEWORK FOR ETHIOPIAN BANKING INDUSTRY

BY

YOSEPH GETU

JUNE, 2021

ADDIS ABABA, ETHIOPIA

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 this thesis entitled "FORMULATING AN INFORMATION SECURITY POLICY FRAMEWORK FOR ETHIOPIAN BANKING INDUSTRY" 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: _____ _____

Yoseph Getu

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

Advisor's Signature: _____ _____ June 4, 2021 _____

Temtim Assefa (Ph.D.)

Acknowledgments

First of all, I would like to thank the almighty GOD who show me this day and beyond. Next to that, I would like to thank all, more specifically the following persons, for your valuable contribution during this thesis work.

My heartfelt gratitude goes to my Advisor, Temtim Assefa (Ph.D.), who also acts as a mentor and instructor, for his energetic and motivating advice, invaluable support, and very important comments.

I am also thankful to my mom Huluageresh, my brothers Samson and Henock, and my sister Selam and her husband Teddy for your continual love and support that make me who I am today.

I would like to thank my wife Yal for your love and support.

I take this opportunity to thank all the financial sector staff, especially the IT departments, for being cooperative in this study.

Finally, my families, friends, classmates, and colleagues who support me indefinitely from start to finish, especially Yalem for opening your door, Gashe Bahru and Yewelsew for your kind support, my in-law's Fasika, Efi, Yordi, Efeson, and Yibe, my brothers Samson and Henock for your advice and genuine feedbacks, Milki and my best friend Robel for your dedication and commitment, and giving me feedback.

Dedication

I dedicate this thesis to God Almighty, my creator and mother Mary, my strong support, my source of inspiration, wisdom, knowledge, and understanding.

Abstract

Today's organizations rely heavily on information and information technology (IT) for the mere function of business operations and stand out from the competition, especially for an organization like banks, as they acquire sensitive data. So these data must be protected at all times against any type or form of attack. Organizations fall victim to such attacks from poorly crafted, redundant, and weak information security policies (ISPs).

This study aims to answer the research question; what are the core values needed develop an information security policy for the Ethiopian banking industry? Furthermore, this can help to determine what security issues exist and the weaknesses and vulnerabilities of the organization. The study explored international information security governance frameworks and best practices; and choses ISO audit checklist, combined with the researcher's experience to develop the framework.

The researcher employed a qualitative research approach. Both primary data; through interviews and secondary data; document analysis are collected and used. A thematic analysis method is used in this research for analyzing the data. To analyze the data QDA MINER lite v2.0.8 tool is used.

Twenty four (24) core elements (codes) under ten (10) master themes; management of security, Acceptable use, data classification level, physical/environmental security, intellectual property right, protection of malicious software, continuity of operations, contracts of employment and services, information asset management, and Access control are identified. The study findings show that the core elements availability in the surveyed banks vary. Furthermore, they are at different position in handling the security of their systems. An entry-level ISP framework is formulated and evaluated. The framework will be the basis of the organizations IS program and serve as a guideline for creating an ISP.

Keywords: Information security, Information security policy, Information security policy development, multiple case study, thematic analysis

Table of contents

List of tables

List of figures

List of Acronyms

CBE	Commercial Bank of Ethiopia
CBS	CORE Banking Solution
CCTV	Closed Circuit Television
CIA	Confidentiality, Integrity and Availability
COBIT	Control Objectives for Information and Related Technology
E-mail	Electronic mail
ICT	Information communication technology
IS	Information Security
ISO/IEC	International Organization for Standardization/International Electro Technical Commission
ISP	Information security policy
IT	Information Technology
IPS	Intrusion Prevention System
LAN	Local Area Network
NBE	National Bank of Ethiopia
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Security Standards Council
PSS	Premium Switch Solutions
QDA	Qualitative data analysis

CHAPTER ONE

INTRODUCTION

This chapter introduces the research background, statement of the problem, research questions, and the research objectives. Furthermore, the chapter describes the significance of the study and the scope of the research.

1.1 Background of the research

Today more than ever, organizations rely heavily on Information and Information Technology (IT) as IT supports their everyday activities and various other critical business functions. Doughty and Grieco (2005) define it as "IT should be viewed as a method for increasing the speed, accessibility, and comprehensiveness of information that supports the decision-making processes within the organization." However, unfortunately, IT dependency has led to increased potential threats to organizations' information assets. This threat is even more high risk for organizations like financial institutions. Akinlolu A. (2007), states "The application and implementation of IT policies have become very important to all banks and a prerequisite for local and global competitiveness."

The literature contains several definitions for an information security policy (ISP). Chen and Li (2014) discuss that an ISP has been deployed by management to distinguish between employee behaviors that are either permissible or prohibited and the accompanying sanctions if the prohibited actions materialize. Contrarily, ISO/IEC 27002 (2013) states that an ISP intends to provide management with direction and support per business specifications, needs, and regulations when overseeing information security (IS). As highlighted in these two definitions, it is clear that an ISP contributes considerably to an organization's well-being when protecting its information. However, the processes involved in developing and implementing an effective ISP are complicated at best.

Von Solms et al. (2011) stresses the importance of ISP as the primary control to mitigate IS threats. Besides, organizations should implement an ISP based on the strategic, tactical, and operational management levels. Top managers should first initiate security policies. Furthermore, it is essential to note that organizations must consider the regulations applicable to that specific organization before writing a security policy (Avolio et al., 2007).

As IS is about protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction; yet information security management (ISM) has been tasked with protecting electronic and non-electronic information assets against the risks of loss, misuse, damage, and disclosure or corruption (ISO/IEC 27002, 2013). Bayuk (2009) emphasizes that the importance of ISM and policy control is one of the first steps in building an influential IS culture.

Although the formulation of ISP starts with designing or assessing the organizations' IS culture, organizations should also focus on procedures and implementation items rather than on the policy documents only (Hong et al., 2006). Because there are different policy audiences in every organization, security policies must consider this issue (National Computer Board, 2011).

Also, Diver (2007) emphasizes the need to consider regulatory requirements before developing security policies. It is essential to consider the current security policy maturity before choosing which approach to follow in developing security policy, as it shall be regarded as the basis for all IS planning, design, and deployment.

According to Munirul U., Zuraini B., & Zailani M. (2011), "Information system has become the heart of modern banking in our world today, and information has become the most valuable asset to protect from insiders, outsiders, and competitors." Banks and customers are anxious about their security state, and as such, they are considering it as one of if not the one top requirement.

Attacks of different likes and from multiple directions can cause havoc to banks, from compromising customer information details to losing credibility and trustworthiness for such organizations. As Bogale (2018) states, for organizations, like a financial institution, securing information is not a choice but a matter of existence. One way to ensure this is by formulating and implementing an ISP; if not, the writing is on the wall.

1.2 Statement of the problem

A vital asset of an organization like a bank nowadays is its information thus must be protected from its formulation to dissemination (Tebkew, 2013). This kind of protection helps banks build trust with their customers as it is believed adequate security builds trust and that the perception of good security and confidence will increase usage.

According to Woretaw and Lessa (2012), one of the swiftly advancing Ethiopian sectors is the banking sector. Though the banking industry is undergoing fast progress in migrating its major business processes towards IT-based services, IS awareness in the Ethiopian banking sector is still unsatisfactory.

On the other hand, Alageel (2003), argues that the human factor also needs to be considered and just as important. Organizations nowadays heavily invest in technical solutions like firewalls and intrusion detection systems but overlook the most vulnerable security factor, which is the human factor. Any attack on an organization and its information comes through humans, which are the weakest link. Numerous attacks could have been prevented if the people involved had been exposed, alert, and aware of IS (Amare, 2015). To address the rise in IS threats, not solely technical solutions like antivirus package tools, however, conjointly information management strategies and policies are put forward (Alageel, 2003; Amare, 2015).

However, as Balcha (2013) pointed out, the IS issue is an issue that technology cannot solve solely and an issue for management to address. Therefore, legal frameworks in

policy and standards are the primary prerequisites to establish efficient and reliable security governance systems. Organizations instinctively move towards technical and procedural security measures to secure information assets and reduce the risk associated with these systems. Although these measures help improve IS, Straub (1990) implies that relying on them alone is not enough to eliminate risk.

Developing and implementing an efficient ISP is not straightforward but is drive by multiple issues such as regulatory requirements, the complexities of new technologies, and external and internal threats (Diver, 2007). The existing literature highlights particular ISP development and implementation methods as stated by (Annad, 2019) but these methods do not include a comprehensive, integrated method that details step-by-step processes.

Latham (2013) states that for the organization's ISP to be helpful, policy documents must be developed that fit the organization's culture. It is essential to support all the critical players in policy development, such as senior management, legal, employees, and system administrators. Due to weak ISP's organizations fall victim to active and passive attacks. Other factors that impede these ISPs are IT users and cause organizations to be under constant information security threats because people unconsciously disrupt these ISPs due to a lack of awareness about related terms, focus areas, and conditions are increasing the risk of IS attacks (Alqahtani, 2018).

Given this lack of guidance, such policies often use those developed by similar organizations, commercially available sources, or templates offered from public sources such as the Internet. However, the document that results from such sources will not provide appropriate guidance for the IS within the organization's context that it is allegedly to protect. McKenna (2010) states that several IT security personnel regrettably do not understand the business risks of writing these huge security policies, so they develop policies that are all about protecting everything.

In the case for the Ethiopian banking industry, almost all of the organization possess some kind of document regarding information policy. But these lack organization, content that that they don't actually implement and coincides with international standards. Much of this comes from the sudden need to comply quickly with a regulatory requirement or a certain compliance standard.

In such circumstances, the policy statements developed might not provide solutions to the problems they are designed to annul, and thus they will not combat the security threats that the specific organization is facing.

There is an abundance of security policy-in-a-box products on the market. This can be a bit daunting, and many organizations are put off by the effort required to gain accreditation and the perception that it can be challenging to implement, and just a few of them will be formally agreed upon by top management unless explained by a security professional (Tuyikeze and Flowerday 2014). As a result, it is not likely to happen due to time constraints ingrained in executive management. If a security professional instead provides mandates to executive management to sign off, management requirements are likely to be overlooked. Even if it was possible to have management endorse an off-the-shelf policy immediately, it is not the right approach (Tuyikeze and Flowerday 2014).

While it is advisable even recommended to refer to international security standards, they are inherently generic. So they must be incorporated into the current structure of the target organization with management input to produce a policy outline. Some of the policy elements found in the frameworks mentioned above are not yet applicable within the context of our country's organizations' technology development. Accordingly, this paper tries to fill this gap by identifying these elements and proposing an entry-level ISP framework. The framework will be the basis of the organizations IS program and serve as a guideline for creating an ISP.

1.2 Research question

- What are the core values needed develop an information security policy for the Ethiopian banking industry?

1.3 Objective

1.3.1 General Objectives

The general objective of this study is to formulate ISP framework for the Ethiopian banking industry.

1.3.2 Specific objectives

The study has the following proposed specific objectives:-

- ✓ Review existing international ISP standards and frameworks,
- ✓ Develop an entry-level ISP framework for commercial banks,
- ✓ Establish a guideline for creating an ISP.

1.4 Significance of the study

The findings from the study has a significant contribution to both academic researchers and practitioners. Academic researchers could be benefited from the theoretical contribution since it tries to fill the existing literature gap, particularly on ISP for Ethiopian banks' settings.

The study helps develop a theoretical proposition or framework on how the administrators should apply and follow the guidelines. The theoretical recommendations provide an excellent insight into how similar sectors of our country should operate to ensure standardization of information system security policy and procedures beyond the successful formulation.

National Bank decision-makers are the primary practitioners that use the proposed framework as a guideline to enforce necessary security policies to increase efficiency. Since they are policy enforcers, they can use this as an outline to direct others to comply. It also serves as a benchmark for practitioners and researchers who want to conduct more research in the ISP area in Ethiopian financial institutions.

1.5 Scope and limitations of the study

The proposed study assess the applicability of the ISP elements in the Ethiopian banks using existing international security standards and propose an entry-level framework. Specific banks are selected as a ground case to be investigated located in Addis Ababa.

The other limitation of the study was that a pilot study was not conducted before the actual research interviews. The intent was to locate an IT manager or security professional who has worked on the policy development and implementation projects. However, because respondents were more challenging to find and time constraints ingrained in top management, it did not pan out as the researcher anticipated.

However, it was known that some interview questions might be modified during the actual interviews. This flexibility supported the semi-structured, qualitative interview methods that had been selected for data collection.

1.6 Operational definitions

For the purpose of this thesis, the following terms and definitions apply.

- Asset - anything that has value to the bank.
- Entry-level – refers to the basic and core values that organizations can be used as a starting point in developing their security program.
- Security- is the degree of protection against danger, damage, loss, and crime.
- Risk- A possibility that a threat exploits vulnerability in an asset and causes damage or loss to the asset.

1.7 Organization of the study

The paper is organized into six chapters. They are;

Chapter One: This chapter has an introductory chapter that provides an introductory and background need for organizations' ISP/standard, especially for financial institutions. It also includes the statement of the problem, objectives of the study, the research methodology used for the research, the study's significance, and the study's scope and limitations.

Chapter Two: This chapter's literature review of IS, related concepts and models, and directly related works have been discussed.

Chapter Three: this chapter presented research methodology, which includes general insight on the existing research methods, what research method was employed in this thesis and why? The sample selection for the study, data collection techniques, and data analysis methods was stated clearly.

Chapter Four: This is the data presentation, analysis, and discussion part. It tries to present the data collected from banks, discuss the research questions, and present the research outcomes.

Chapter Five: This chapter presents the proposed information security policy framework for Ethiopian banking industry based on the findings of analysis of the research and reviewing existing security governance frameworks.

Chapter Six: The last chapter is about the study's conclusions, recommendations, and future works.

CHAPTER TWO

LITERATURE REVIEW AND RELATED WORKS

This chapter's literature review of IS, related concepts and models, and directly related works has been discussed.

2.1 Literature review

2.1.1 Information Security

Lately, IS has received much attention because the information is one of a financial institution's most important assets, and protecting it is necessary to build and sustain trust between the service providers and its customers Pang M. (2017). Properly designed and implemented IS plays a vital role in securing organizational data and provides data storage methods. With a growing demand for IS, many have stressed the importance of eliminating risks, which are apparent in many organizations (Kadam, McGlasson 2007) and Von Solms, 2006).

Douglas (2011) advises that organizations need to identify the assets to be protected during the risk assessment stage and assess the threats and vulnerabilities. IS is about protecting things that are of value to an organization. That includes property, people, and data; simply put, the organization's assets. It is essential to involve employees in asset identification, as assets include the employees of computer use. As the access to computer-stored data has increased, IS has become significant (Tse et al., 2013).

Security controls are there to reduce or mitigate the risk to those assets. They include any policy, procedure, technique, method, solution, plan, action, or device designed to help accomplish that goal. Common examples include firewalls, surveillance systems, and antivirus software NIST.SP.800-53rd (, 2013). According to NIST, one way of classifying controls is by type: physical, technical, or administrative, and by function: preventative, detective, and corrective.

Control Types

- ✓ Physical controls- instruments used to detect or prevent unauthorized access to organizational assets.
- ✓ Technical controls- include hardware or software mechanisms used to protect assets.
- ✓ Administrative controls- refer to policies, procedures, or guidelines that define personnel or business practices per the organization's security goals.

Control Functions

- ✓ Preventative controls- put forward any security measure design to stop unauthorized or unwanted activity from occurring.
- ✓ Detective controls- describe any security measure task has taken or solution implemented to detect and alert unauthorized activity during or after it has occurred.
- ✓ Corrective controls- include any measures taken to repair the damage or restore resources and capabilities to their initial state following an unauthorized or unwanted activity.

Table 1. Below shows examples of the abovementioned items classified by control, type, and control function.

Table 1. Control type and function relationship

		Control Type		
		Physical	Technical	Administrative
Control Function	Preventive	Locks, fences	CCTV	Repair physical damage
	Detective	Firewall, antivirus software	Intrusion detection systems	Patch & reboot a system
	Corrective	Separation of duties, data classification	Review access rights, audit logs	Implement business continuity plan, incident response plan

According to Jones (2010), information assets' security is a requirement for all organizations to protect the business or meet legal or regulatory requirements. Organizations are dependent on their IT systems to capture, store, process, and distribute company information. Practitioners and developers use a combination of security controls based on stated control objectives tailored to the organization's needs and regulatory requirements. Ultimately, the goal controls are to uphold the three

foundational principles of security: confidentiality, integrity, and availability, and for this, IS is and has always been the discipline to mitigate the risks impacting the company's IT resources (Von Solms, 2006).

IS refers to protecting or safeguarding sensitive information and information systems from unauthorized access, disclosure, modification, disruption, and destruction ISO/IEC 27001 (2013). It is how an organization protects and secures its systems and facilities that process and maintain information vital to its operations. It is merely the process of keeping information secure, protecting its availability, integrity, and privacy. Furthermore, ISO/IEC 27001 (2013) state that IS emphasizes confidentiality, integrity, and availability; and proposed the CIA triad model, shown in Figure 1.

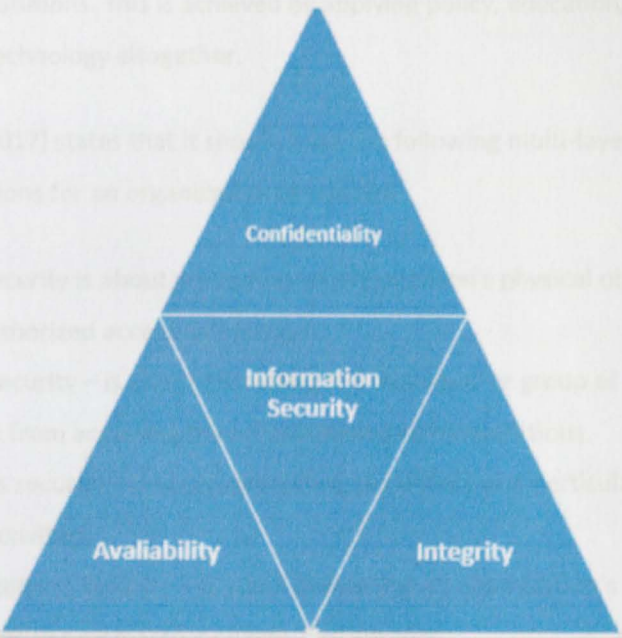

Figure 1. CIA Triad

According to ISO/IEC 27001 (2013), IS includes three components;

- ✓ Availability – is the affirmation that information, assets, and resources are available only to those authorized.
- ✓ Integrity – is described as protecting information, application, system, and network from unauthorized change, be intentional or accidental.
- ✓ Confidentiality – is about privacy, integrity to upholding the constancy, and availability to 24/7 data access.

For most organizations, information is a critical resource to be secured. It is even more so in financial institutions. This is achieved by applying policy, education, training and awareness, and technology altogether.

Gebrehawariat (2017) states that it should have the following multi-layers of security to protect its operations for an organization to succeed.

- ✓ Physical security is about protecting an organization's physical objects or areas from unauthorized access and misuse.
- ✓ Personal security – is about protecting the individual or group of authorized individuals from accessing the organization and its operations.
- ✓ Operations security – is about protecting the details of a particular operation or series of activities.
- ✓ Communications Security – is about protecting an organization's communications media, technology, and content.
- ✓ Network security – is about protecting networking components and connections.
- ✓ IS – is about protecting the confidentiality, integrity, and availability of information assets while in storage, processing, or transmission.

At the most fundamental level, IS is about protecting valuable things to an organization. That generally includes people, property, and data generally referred to as an

organization's assets. Security controls exist to mitigate the risk to those assets. They include any policy, procedure, technique, method, solution, plan, action, or device designed to help accomplish that goal Gebrehawariat (, 2017).

Ousley (2013) states that organizations may have confidential information, ranging from customer lists to financial forecasts and the like, which intended for internal use. Loss or theft of this confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company. Furthermore, Ousley (2013) continues, these types of information must only be available to external audiences for business-related purposes or after entering a nondisclosure agreement.

2.1.2 Information Security governance

According to Posthumus and Von Solms (2004), IS governance is defined as a series of actions on how IS can be dealt with at an executive level. IS, which involves protecting the confidentiality, integrity, and availability of organizational information, reduces the different risks that can harm business information by applying appropriate security controls. For organizations to effectively implement a suitable set of controls and manage IS effective, various security requirements and guidelines need to be considered. These security requirements and guidelines originate from sources, both internal and external, to an organization.

It is crucial to address both internal and external security requirements to manage suitably IS and prevent possible consequences of any negligence in IS. These security requirements contain requirements to secure the IT infrastructure, legal, regulatory and statutory requirements, and requirements for information confidentiality, integrity, and availability as recognized by the organization. Together with the guidance of accepted security standards, such as ISO/IEC 27 series and other best practices, these requirements create the base of a practical approach to IS (Posthumus & Von Solms, 2004).

Regarding external requirements and guidelines, the IS standards and best practices are crucial as they inspire global IS principles and help develop relationships between organizations and their stakeholders. ISO/IEC 27 series is an example of such a standard that guides how organizations can deal with IS by providing IS advice based on ten broad security control categories. The standard is considered as a starting point for organizations to start an effective IS strategy. Governments worldwide have decided to create numerous statutory and legislative requirements to motivate, encourage, and improve corporate IS efforts. There is a different kind of legal requirements that organizations are supposed to comply with. These contain different discipline-specific and also country-specific statutes and laws (Veiga & Eloff, 2007).

Concerning internal requirements, IT infrastructure issues connected with IS help describe requirements to secure the crucial infrastructure that constitutes the information backbone. Business information issues combined with IS define relevant requirements for protecting the confidentiality, integrity, and availability of sensitive business information assets. These issues are addressed by making a risk analysis that intends to identify and evaluate different risks. Next, a process of risk management is done, in which appropriate security controls are chosen and implemented to mitigate these possible risks (Veiga & Eloff, 2007).

There are two essential sides to IS governance that help achieve an effective strategy for addressing business information threats at a corporate governance level.

Primarily, there is a governance side, including executive management and the board. They must set the IS direction and strategy, controlling the IS efforts in their organization. By directing an organization's IS efforts, executive management, and the board should create a corporate ISP that demonstrates that they are committed to IS and supports the organizational mission, goals, and IS strategy. In controlling an organization's IS efforts, executive management, and the board must have periodic reports from different organizational department managers to carefully examine and review their strategies and policies to be checked against rules or laws and improved if necessary.

Second, the management side involves how the management and the implementation of an organization's security strategy will be. This includes how different department chefs and other managers are committed to implementing the corporate ISP with conventional security codes. An example of a code of practice is the ISO/IEC 27 series, which provides proper security controls to protect the integrity, confidentiality, and availability of business information and help integrate IS into an organization's everyday activities and functions (Von Solms, 2005). In general, the implementation of a new standard costs a lot of money. However, organizations will reduce the money spent on IT security operations in the long run.

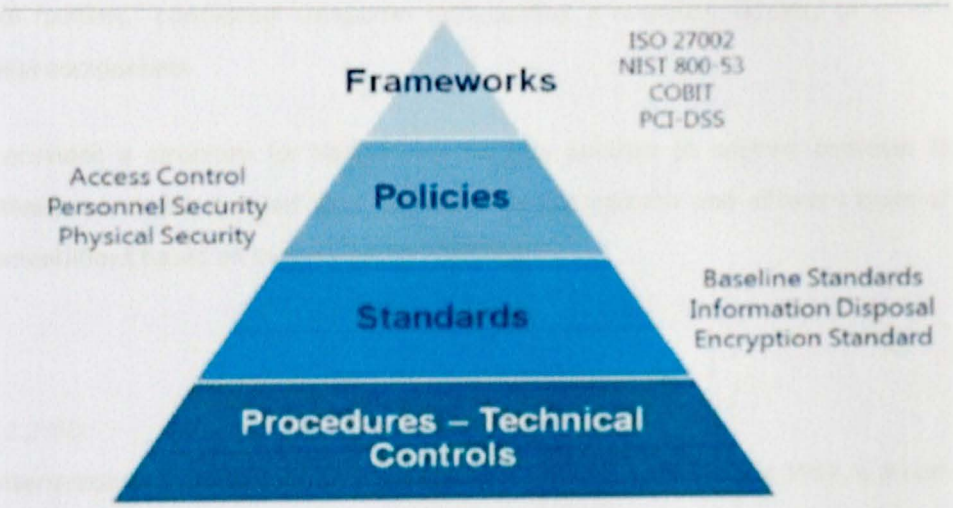

Figure 2. Hierarchy of frameworks, policies, standards, and procedures

It will also improve the security processes, which means the dependency on third-party services will be decreased or even removed. Furthermore, organizations can increase their benefit if their stakeholders understand the need for an IS management system.

2.1.2.1 Information Security governance frameworks

2.1.2.1.1 NIST

The National Institute of Standards and Technology (NIST) provides a set of "Special Publications" to assist the industry, government, and academic organizations with following best practices. The "800 series," the set of security-specific publications, is particular to individual technologies, except 800-53. 800-53 was developed primarily for the US Federal Government to specify security control organization and structure, security control baselines, standard controls, security controls in external environments, security control assurance, risk management, information system categorization, security control selection, and monitoring of security controls. It is organized into 18 "security control families," conceptual categories representing a complete security program's essential components.

NIST provides a structure for considering security controls to address common IS objectives. It includes detailed descriptions of specific controls and different types of implementations based on security categorizations.

2.1.2.1.2 ISO

The International Organization for Standardizations (ISO), established in 1947, is a non-governmental international body that collaborates with the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU) on ICT standards. The ISO 27000 series of IS standards provide frameworks for developing a security program from concept to maturity. It has broken up into several parts to be manageable, and each part prescribes a set of activities that belong to phases comparable to those in the Plan-Do-Check-Act (or more accurately, Plan-Do-Check-Adjust) (PDCA) cycle.

The certification of ISO 27001 gives extra security to the existing IS system without changing the structure of IS processes. ISO 27001 preserves confidentiality, availability,

and integrity as the critical principles in its standards. The application of ISO 27001 standards can be beneficial to organizations. It can facilitate establishing a rigorous framework that provides security to the organization and the information assets. The standard ISO 27001 can help evaluate, implement, and maintain an IS management system (Abu Talib et al., 2012).

The ISO/IEC 27000 series is a comprehensive set of controls, including best practices in the IS paradigm. It is recognized internationally, broad in scope, and generic inapplicability, focusing on risk assessment, identification, and management issues.

Its business goals are:

- ✓ Ensure business continuity
- ✓ Minimize business damage
- ✓ Maximized return on investments

2.1.2.1.3 COBIT

COBIT is a set of IT management practices published by the Information Systems Audit and Control Association (ISACA). ISACA is a universally recognized independent IT governance organization, and its COBIT guidelines are used by IT management in various organizations to define and manage processes based on a maturity model like the Capability Maturity Model (CMM). COBIT is not about IS, it is a general IT standard, but absolute security practices are embedded within it.

COBIT 5 is the current version organized from five conceptual areas Plan, Do, Check, Adjust, and Governance. It includes best practices, processes, and measures an organization can implement to standardize IT management. It is generally considered complementary to ISO/IEC 2001 and 27002.

2.1.2.1.4 PCI DSS

PCI-DSS is one of the worldwide IS standards defined by the Payment Card Industry Security Standards Council. The standard was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI helps organizations process card payments and prevents credit card fraud through increased controls. It serves as a baseline of technical and operational requirements designed to protect cardholder data. It can apply to all organizations that hold, process, or exchange cardholder information. PCI Data Security Standard Requirements and Security Assessment Procedures combine the twelve requirements and corresponding testing procedures into a security assessment tool. PCI DSS is designed for use during compliance assessments as part of an entity's validation process.

Usage of payment cards such as debit cards, credit cards, and prepaid cards continues to grow. Security breaches related to payment cards have led to billion-dollar losses annually (Jing Liu, 2010). To offset these, the PCI-DSS, the first industry-wide standard that aims to achieve strong protection of sensitive consumer and cardholder data, prevents significant security issues. It is founded by the collaborative effort of the major payment card networks and issuers, including the standard, sets forceful requirements in many aspects, including secure networks, cardholder data protection, access control, vulnerability management, security assessments, and reporting (Liu et al., 2010). Unlike the other significant security standards like ISO, PCI-DSS focuses on protecting cardholder information of financial organizations, including card service issuer and acquirer.

If financial institutions get compliant with PCI-DSS, they can provide effective international card payment services locally. According to Ataya (2010), one of the significant advantages of this standard is, Issuers and Acquirers of Payment cards are no longer required to follow up to four separate programs (Visa, MasterCard, American Express, and Discover) that were applied differently in each region or country of operation

for each credit card if the merchant or service provider has passed the PCI-DSS and standard requirements.

A hierarchy of risk-based policies, standards, and operating procedures imposed by PCI-DSS requirement lay down key IS directives and mandates for the entire organization to promote a risk-aware culture (Ataya, 2010). To that end, PCI-DSS has twelve major requirements divided into six categories, as shown in table 2. Each requirement has sub-requirements, and some have sub-sub-requirements (Morse and Raval, 2008).

Table 2. PCI-DSS twelve requirements; adapted from PCI-DSS Reference Guide (2010) (cited by G/Hawariat).

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS is applicable in current Ethiopian PSS member banks: Awash International Bank, United Bank, Nib International Bank, Addis Bank, Berhan Bank, and Cooperative Bank of Oromia. These banks have to comply with the PCI DSS standards and requirements.

Though all information security governance frameworks have Information Security Policies, Procedure, and Standards as one of the most basic requirements, the researcher

adopted ISO audit checklist because it specifies requirements for the implementation of security controls customized to the needs of individual banks.

2.1.3 Information Security Policy

ISP is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets, and makes future decisions about its information systems security infrastructure NIST (2003). It paints an organization's complete security architecture picture, and the document includes clear objectives, formal procedures, goals, rules, and regulations. It mentions the assets to be protected and the person who can log in and access data, who can view the selected data, and the person who is allowed to change the data. Without these policies, it is impossible to protect the company from possible threats NIST (2003).

According to Peltier (2005), the policy describes security roles and responsibilities, the scope of information that needs to be protected. They should not state precisely the proper operation of software or equipment. This kind of information should be stated in other documentation called standards, procedures, guidelines, and practices. Figure 3 shows the relationship between policies, standards, and guidelines.

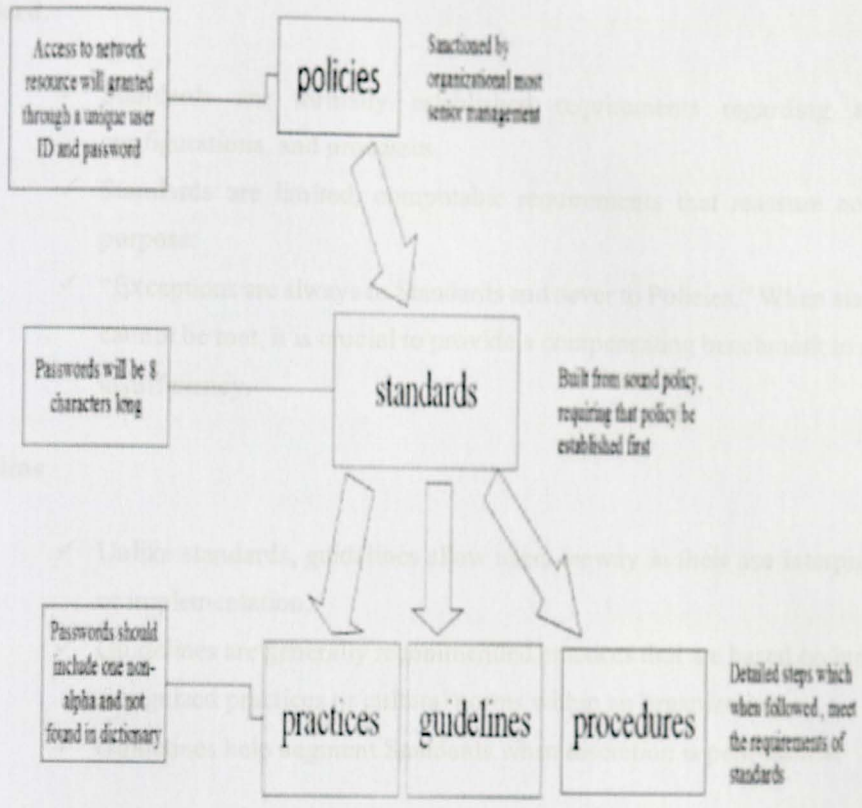

Figure 3. Policy development structure

Source: Whitman & Mattord, 2014

Policy.

- ✓ A policy is a "high-level management intent statement that formally establishes requirements to guide decisions and achieve rational outcomes."
- ✓ A policy is a statement of intention that is imposed by standards and further executed by procedures.
- ✓ External factors, such as regulatory or contractual obligations, are commonly the root cause of a policy's existence.

Standard.

- ✓ Standards are formally established requirements regarding actions, configurations, and processes.
- ✓ Standards are limited, computable requirements that reassure control's purpose.
- ✓ "Exceptions are always to Standards and never to Policies." When standards cannot be met, it is crucial to provide a compensating benchmark to reduce insufficiency.

Guideline.

- ✓ Unlike standards, guidelines allow users leeway in their use interpretation or implementation.
- ✓ Guidelines are generally recommended practices that are based on industry-recognized practices or cultural norms within an organization.
- ✓ Guidelines help augment Standards when discretion is permissible.

Bayuk (2009) posits that the formulation of an ISP should begin with top management. Accordingly, high-level security policies emerging from the executive management are disseminated from the strategic level to the tactical level, translating into standards or guidelines. Finally, they are distributed to the operational level in procedures (Von Solms et al., 2011). During the policy formulation stage, management involvement is essential because it must approve the security policy. Likewise, Kadam (2007) advises that employees need to create a sense of ownership when developing an ISP. It is also critical to start preparing employees for the upcoming changes and coping with the new policy requirements. Involvement is critical in moving users through the stages of commitment, emanating from preparation through acceptance and ultimately to the commitment stage.

Maynard et al. (2011) further suggest that the end-users and external representatives, such as customers, suppliers, and other external entities, be included in developing an ISP to ensure its multidisciplinary nature. This involvement by end-users should occur at an early stage so that they are allowed to identify errors, which may then be fixed before the security policy implementation. "If the policy documents are hard to follow, users may not read them fully or fail to understand them accurately, thereby unnecessarily risking security compromise" (Diver, 2007). Therefore, the inclusion of multiple stakeholders in developing an effective security policy is crucial because it gives the organization a sense of ownership of the security policy, facilitating the acceptance and adoption of Maynard et al. (2011).

For an ISP to live on and attain its objectives, management, employees, and stakeholders need to support the entire process of developing and implementing it. The development of an effective security policy needs a combination of skills that emerge from the different stakeholders' experiences (Diver, 2007).

2.1.3.1 Purpose of Information Security Policy

The primary purpose of the ISP is to provide a better security environment. An acceptable security policy should outline individuals' responsibilities, define penalties for violations, and provide a mechanism for updating the policy Diver (, 2007). IS should be assessed and revised regularly. As shed light by Talbot and Woodward (2009), one of ISP monitoring and assessment objectives is to produce measurable results that show users' behavior. These results should then be used to evaluate the users' performance in terms of security policy compliance. During an audit of security policy compliance, users that demonstrate high-security policy compliance should be encouraged and rewarded. On the other hand, those who violate the organization's ISP should be cautioned and penalized.

SANS (2009) posits well-written policy will provide guidelines on what acceptable use and prohibited use are, which will automatically reduce risks if employees abide by the policy.

They can serve as a pedestal for conducting audits of the network and its resources, serving as a guideline to follow when conducting forensics activities if security has been breached. ISPs often provide the framework for the prevention, detection, and response to security breaches. The policy document typically is supported by standards that tend to have a more technical or operational focus SANS (, 2009).

According to Diver (2007), a security policy should fulfill many purposes. It should:

- ✓ Help shield information and people (organizational assets)
- ✓ Help set the rules for expected behavior by users, system administrators, management, and security personnel.
- ✓ Help minimize risk
- ✓ Help track compliance with regulations and legislation
- ✓ Authorize security personnel to monitor, inquiry, and investigate
- ✓ Define and authorize the consequences of violation

Diver (2007) stated that policies must be useable, workable, and realistic. It is essential to involve and commit from major stakeholders in policy development and support such as senior management, audit and legal, and those who will have to use the policies as part of daily work. Other essential elements to achieving these are communicating the importance and usefulness of policies to those who have to live with them.

2.1.3.2 Fundamentals of Information Security Policy

According to Joel et al. (2001), a security policy should be "economically feasible, understandable, realistic, consistent, procedurally tolerable, and provide reasonable protection relative to the stated goals and objectives of management." They explain the overall security and risk control objectives that an organization endorses. Joel et al. (2001) stressed that an acceptable security policy should have the following characteristics.

- ✓ Implementable
- ✓ Enforceable with security tools

- ✓ Define areas of responsibility for the administrators, employees, and management.
- ✓ Documented, distributed, and communicated.

Formulating an effective security policy and taking steps to ensure compliance is a critical step to prevent and mitigate security breaches. To make security policy truly useful, update it in response to changes in the organization, conclusions drawn from previous breaches, and other security posture changes. Without policies, an organization's security program will be numbered SANS (2002). The ISP must be practical and enforceable. It should have an exception system to accommodate requirements and urgencies that arise from different organization parts. An info security policy can be as broad as everything related to IT security and related physical assets' security but enforceable in its full scope.

According to (Joel et al. 2001), the following list offers some essential considerations when developing an ISP.

Roles and Responsibilities

The participation of various organizations dictates the development of security policies. Appoint staff to education, change management, incident management, carry out user access reviews, and periodic updates of the security policy. Responsibilities should be clearly stated as part of the security policy.

Audience

In addition to determining the roles and responsibilities of those involved in developing security policies, the security policies' intended audience must also be considered. Primary, determine if policies are internal or external or both; then determine the audiences' orientation by topical areas such as management (business or technical) employees, temps, contractors, customers or clients executive.

Purpose

First, define the purpose of the policy, which may be to:

- ✓ Create an overall approach to IS.
- ✓ Detect and defend IS breaches such as misuse of networks, applications, data, and systems.
- ✓ Keep the reputation of the organization, and uphold ethical and legal responsibilities.

Goals

The goal is to act as a bridge between management objectives and specific security requirements. It is to guide the management team to agree on well-defined objectives for strategy and security.

Flexibility

The policy must be flexible in order to be successful. It should be independent of specific hardware and software decisions, as their specification may change rapidly.

Communication

For security and privacy policies and procedures to be effective, they must be communicated to all appropriate users, staff, management, vendors, third-party processors, and support personnel.

Management

Application and relevance of the policy document need to be reviewed and updated in pre-set time lapses. Failure to keep the policy up to date reflects a lack of management's commitment or the failures in organizational governance processes.

Posture

It is a must that every organization has policies in place that support sound business practices, and they will demonstrate to the world that this organization understands that the protection of assets is critical to the successful execution of its mission and its healthy posture. A typical security posture should have confidentiality, integrity, and availability of its assets.

Relationship to Standards and Procedures

For policies to be considered whole, they should be feasible and implementable based on standards, controls, guidelines, and procedures. They present a clear path to all appropriate users, staff, management, vendors, third-party processors, and support personnel. Standards, guidelines, and procedures are only used and defined after developing and accepting security policies (Joel et al. 2001).

According to Negussie (2015), for formulating, developing, and implementing an effective security policy, the following principles should be considered. These are:-

- ✓ Develop policies that we plan to enforce
- ✓ Explain the purpose of the policy
- ✓ Develop security policies that do not require updated frequently
- ✓ Differentiate between policies and standards or recommendations
- ✓ Include employees from other departments in policy development
- ✓ Policies should be available to everyone.
- ✓ Security policies stay up to date.
- ✓ Policies are understood and agreed upon
- ✓ Require acknowledgment of our policies
- ✓ Minimize details (those belong in the procedures)
- ✓ Minimize jargons and use straightforward language
- ✓ Match the corporate culture
- ✓ Do not include it if it cannot be accomplished

2.1.3.3 Types of Information Security Policy

"Different organizations will need different policies for effective security management." (instantsecuritypolicy.com, 2008). Some may need all, while others need only a handful. That said, specific policies can reasonably be considered "essential" to security management and apply to almost every company.

Table 3. Standard organizational security policy.

Essential	Optional
Acceptable Use Policy	Data Classification Policy
Authentication Policy	Outsourcing Policy
*** Backup Policy***	Mobile Device Policy
Confidential Data Policy	Encryption Policy
Password Policy	E-mail Policy Guest
Network Security policy	Physical Security policy
Network Access Policy	Access Policy
Incident Response Policy	Retention Policy
	Wireless Access Policy
	Third-Party Connection Policy
	VPN Policy

The essentials are discussed in detail below according to the ISO/IEC 27000 (2013) and SANS (2009) security governance frameworks:-

Acceptable Use Policy

This policy is used to define acceptable and unacceptable use of information assets. These rules are in place to protect the company's resources from various attacks, including the following.

- ✓ Appropriate use of e-mail and related resources
- ✓ No expectation of privacy
- ✓ Accessing without the user's consent

Authentication Policy

The purpose of this policy is to validate who is attempting to use systems and applications that do have the proper credentials. This can be archived by various authentication methods, including

- ✓ Entering a password into your laptop
- ✓ Entering a PIN into handheld devices or payment cards
- ✓ Entering keys or smart cards (physical)

Backup Policy

The purpose of this policy is to establish a working culture for the backup and restoration of electronic information and information assets.

Confidential Data Policy

The purpose of this policy is to define the method of data classification and procedures for data classification of the organization's information and information system assets

based on its level of sensitivity, value, and criticality. Organizations need to describe the method of information classification. Also, they need to describe the procedures for information labeling and handling performed per the information classification scheme. Classification of data will help define any laws or regulations that apply.

Password Policy

The purpose of this policy is to enforce employees to set a minimum requirement for password usage. Organizations need to describe the password controls in place for operating systems and access to critical applications.

Network Security policy

The purpose of this policy is to have 100% visibility and availability networks. Unless a flat network is used, organizations need to describe how network segmentation, or isolating (segmenting), sensitive systems from the remainder of an entity's network is accomplished.

Network Access Policy

The purpose of this policy is to build rules for using and accessing network infrastructure. These rules allow the administrator to configure the policy to either permit or reject access to users if the connection request matches the conditions and restrictions of the network policy.

Incident Response Policy

The purpose of this policy is to describe the procedures for incident response. The other purpose is to describe the procedures to respond to alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems, including detecting unauthorized wireless access points. The information gathered from these occurrences can be analyzed to continually identify trends and direct efforts to improve and strengthen the information security infrastructure.

Further (Whitman & Mattord, 2014) posit that organizations need to describe three types of ISP to create a complete ISP

a. Enterprise ISP (EISP)

b. Issue-specific security policies (ISSP)

c. Systems specific security policies (Sys SP)

a. Enterprise ISP (EISP)

An enterprise ISP establishes the strategic direction, scope, and tone for its security effort and gives responsibilities for different IS areas. It provides guidelines for the development, implementation, and management prerequisite of the IS program (Whitman & Mattord, 2014).

b. Issue-specific security policies (ISSP)

Issue-specific policies give detailed instructions and guidance to all organization members using a resource, such as a processor technology used by the organization. An organization's ISSP should communicate complex technology-based systems and be updated frequently (Whitman & Mattord, 2014).

c. System specific security policies (Sys SP)

System-specific security policies do not resemble other types of policies. They can often be made to function as standards or procedures used when configuring or maintaining

systems such as configuration and operation of a network firewall (Whitman & Mattord, 2014).

Sys SP can be of two kinds:

• **Management guidance Sys SP**: the managerial guidance Sys SP document is made by the management. It contains guidance for the implementation and configuration of technology, and a description of reasonable behavior that people in the organization should adopt to support IS (Whitman & Mattord, 2014).

• **Technical specifications Sys SP**: the managerial policy is created together with the manager and system administrator; the system administrator may need to make another kind of policy to implement the managerial policy (Whitman & Mattord, 2014).

2.1.4 Information Security Policy Development

The development of ISP is composed of a two-part project: In the first part, the policy is designed and developed, and in the second part, management processes are created to ensure that the policy would continually be used within the company. The policy development projects should be well planned, funded, managed, and be finished on time and within budget (Whitman & Mattord, 2014).

According to Whitman & Mattord (2014), policy development projects can be guided by the security development life cycle process.

The Investigation phase: Here, the policy development team should:

- ✓ Obtain support from senior management (CIO). If the project gets support from the senior management, it has a better chance of success. The more top management gets involved, the easier the implementation will be.
- ✓ Posit the purpose of the policy neatly.

- ✓ Gain participation of the exact individuals who are affected by the recommended policies
- ✓ The team should be composed of representatives from the legal department, human resources department, and the end-users.
- ✓ Assign a project manager to see out the project until the end.

The Analyzing phase: Here, the activities to be included are:

- ✓ Make a new or recent risk assessment or IT audit recording the organization's current IS needs.
- ✓ Collecting essential reference materials, as well as existing policies

The Design phase: This phase should include a plan for how policies should be distributed and how verification of distribution should be achieved. Members of the organization must acknowledge that they have received and read the policy.

The Implementation phase: Here, the policy development team writes the policies. The team has to ensure that policies are enforceable as written documents and distributed, read, understood by those to whom it applies.

The Maintenance phase: In this phase, the policy development team maintains and changes the policy as needed to ensure that it continues to be effective. The policy should be connected to a system via which problems related to it can be reported anonymously. It also should be reviewed regularly.

Developing an ISP document will need a high level of commitment, not just from the IS groups but also from other IS personnel in the organization. For the project will get enough resources, management buy-in must be launched at the start of the policy development project. Management must recognize the policy development project's importance to allocate the later phases (Latham, 2013).

According to Latham (2013), it is essential to communicate the need and the importance of IS policies "to those who have to live by them" to achieve its successful implementation. Sometimes, employees think that policies are going to stand in the way of their everyday work. An essential part of policy development and to make sure the policies are put into practice and not refused by employees is to communicate the information that policies are helpful. This can be done by giving a framework within which employees can work, reference best practices, and obey the legal requirements. Once employees become aware that ISP will help them in their daily work, they would be much more willing to the ISP document and ensure compliance. Similarly, when top management is willing to accept that policy is a tool they can benefit from to help assure devotion to legislative requirements and effective IS management, they may be more engaged and supportive in providing resources.

Top management should support the ISP document from inception to the maintenance process by safeguarding its resulting policies and putting efforts into the implementation process. They should also be ready to support projects that it is caused by policy to assure compliance. This support is vital to the ongoing feasibility of policy development (Latham, 2013).

2.1.5 Information Security Policy Approach

According to Whitman & Mattord (2014), the implementation of ISP can be achieved in two ways: the top-down approach and the bottom-up approach.

Top-down approach: There is coordinated planning from the top management and a committed champion who provides funding and proposes the implementation process. Top management provides sufficient resources, gives directions, and produces policies, procedures, and processes.

Bottom-up approach: - is launched by IT administrators and security professionals. In this approach, systems administrators try to enhance their systems. Systems and network administrators have substantial knowledge that can help to enhance the IS in the

organization. They know the risks that can be harmful to their systems, and they know what mechanisms and policies are needed to secure their systems. This approach is rarely successful because the top management does not coordinate, such as coordination between departments and provision of sufficient budget. The two approaches are presented in figure 4.

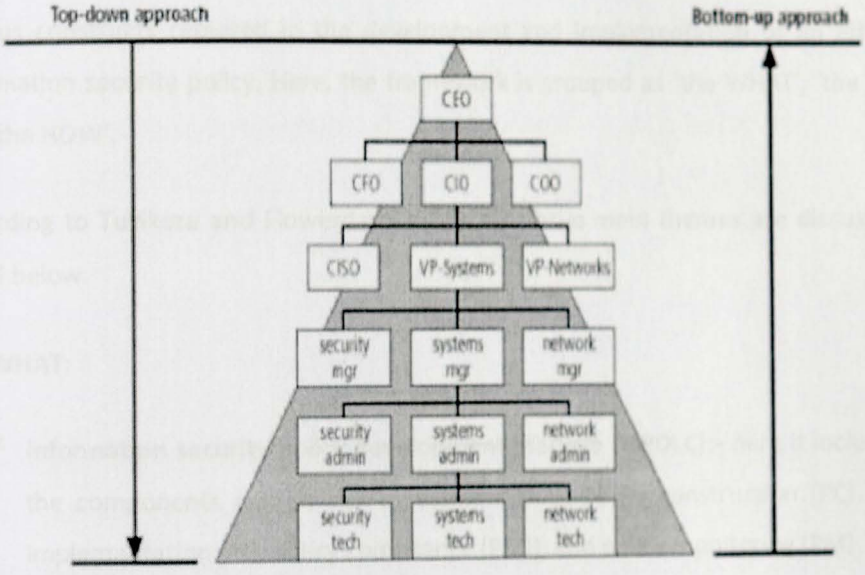

Figure 4. Top-down and bottom-up approaches

Source Whitman & Mattord, (2014)

2.1.6 Information Security Policy stakeholders

An efficient security policy requires various skills emanating from different stakeholders' experiences (Diver, 2007). Maynard et al. (2011) recommend the involvement of ICT Specialists and security specialists in the policy development process because they need technical knowledge of the systems that the knowledge security policy intends to guard because of these systems' security. Diver (2007) posits that the human resource

department should review and approve the safety policy supported by how the policy relates to the organization's existing policies. This is necessary to ensure that there is a consistency between the organization's security policies and quality organizational practices (Maynard et al., 2011). The inclusion of multiple stakeholders is crucial to the organization because it gives the whole organization a sense of security policy ownership and facilitates the safety policy acceptance and adoption.

Furthermore, Tuyikeze and Flowerday (2014) proposed a framework that outlines the various constructs required in the development and implementation of an effective information security policy. Here, the framework is grouped as 'the WHAT', 'the WHO' and 'the HOW'.

According to Tuyikeze and Flowerday (2014), the three main themes are discussed in detail below.

The **WHAT**:

- ✓ **Information security policy development lifecycle (ISPDLC):-** here it includes all the components namely risk assessment (RA), policy construction (PC), policy implementation (PI), policy compliance (PCO), and policy monitoring (PM).
- ✓ **Internal and external drivers: -** The internal threats include insider employees who place the organization's information at risk, while external threats include hackers. In addition, there is the necessity of complying with proliferating government legislative requirements
- ✓ **ISP guidance**: - includes international governance frameworks e.g. ISO, NIST...
- ✓ **Existing theories**: - includes General Deterrence Theory (GDT) for identifying the severity of a punishment and the Theory of Planned Behavior (TPB) to identify intention of an individual to perform a task.

The **WHO:**

- ✓ **Executive management**: - management plays a significant role in organizational decision-making process.
- ✓ **End users**: - who perform various activities in an organization.
- ✓ **Legal council**: - who provides information on current laws as well as anticipated legislative requirements.
- ✓ **Technical staff**: - experts who can guide the development team as consultants.
- ✓ **Human resource**: - to ensure that the security policy is in line with standard organizational practices.
- ✓ **External representatives**: - such as customers, suppliers and other external entities.

The **HOW:**

The how is described as the relationship b/n these constructs. The findings of the inferential statistical data analysis showed a positive correlation between Management Support and the ISPDLC, with a statistically significant result. It also revealed the existence of a significant relationship between Employee Support and the ISPDLC constructs.

2.2 Related works

N	Author	Paper contribution
1	Amare (2015)	The objective of this paper is to examine the insider threat of the Ethiopian banking industry. It identified insider threats and motivations within the Ethiopian banking industry recommends best

		practices to mitigate those insiders' malicious activities within the Ethiopian banking sectors.
2	Avolio et al. (2007)	This paper explains the processes involved in writing a security policy to protect network security. It emphasizes that top managers should initiate security policies. Furthermore, it put forth that, before writing a security policy, organizations must consider the regulations applicable to that specific organization.
3	Diver, (2007)	This paper offers a unique perspective on the need to consider regulatory requirements before developing security policies. The paper also recommends considering the current security policy maturity before choosing which approach to follow in developing a security policy.
4	Hong et al. (2006)	The finding of this paper highlights that organizations should focus on procedures and implementation items rather than on the policy documents only.
5	Khan (2010)	This paper emphasizes the importance of ISP communication and publication within an organization. Also, it discusses the need for detailed process documentation of an IS program.
6	Negussie (2015)	The purpose of this paper is to assess IS and ISP practices and to identify the challenges and prospects of ISP in the Ethiopian banking industry

		and, therefore, proposed recommendations in formulating and implementing ISP.
7	(Tebkew, 2013)	This paper aims to propose and develop an IS management framework in Ethiopia's banking industry.
8	Von Solms et al. (2011	This paper discusses the importance of ISP as the primary control to mitigate IS threats. The paper also highlights how the ISP should be implemented based on the strategic, tactical, and operational management levels.
9	(Woretaw & Lessa, 2012)	The purpose of this paper is to assess the current IS culture and identify critical problems. Thus, practitioners can implement recommended measures to enhance the IS culture in the banking sector in Ethiopia.
10	InstantSecurityPolicy.com (2013)	This paper discusses the integration of security policy formulation processes with a business management model in terms of which the security risks may be easily quantified.

2.3 Summary

An ISP should reflect the organization's objectives, and every stakeholder should be a part of it. The policy to help execute the program's remainder should also be formally agreed upon by executive management. To formulate an ISP document, the organization needs to have well-defined objectives, goals, and an agreed-upon management strategy for securing information.

If there are disputes over the policy's content, then the disputes will continue throughout successive attempts to enforce it, with the outcome that the IS program itself will be dysfunctional.

A decent enough ISP can make the difference between a growing business and an unsuccessful one. Identifying the type and levels of security required and defining the applicable IS best practices are enough reasons to back up this statement. If we want to lead a prosperous company in today's digital era, we certainly need to have a good ISP.

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter discusses the research design and techniques used to answer the research questions. Hence, the researcher discussed the research approach and method, research area and population, sampling technique and data collection instrument, analysis, and trustworthiness.

3.1 Research design

Yin (2003) noted that "the research design is a technical plan that attempts to link the beginning and end of a study (cited in Cater-Steel & Al-Hakim, (2009)). The research design facilitates research to be as efficient as possible in terms of effort, time, and cost. Kothari, (2004). The research is exploratory research, which tries to identify the various core elements needed to formulate an ISP framework regarding the Ethiopian banking industry.

3.1.1 Research approach

Creswell (2013) describe research approach as a roadmap for research that range from vast assumptions to detailed methods of data collection, analysis, and interpretation. The two basic approaches to research are quantitative and qualitative, without leaving a mixture of both. Qualitative approach tries to explore attitudes, behavior and experiences through such methods as interviews or focus groups while quantitative approach involves the generation of data in quantitative forms (Dawson, 2002).

The study adopted a qualitative approach, which helped identify the existing theories and methods for formulating a standard ISP. The researcher has done this by reviewing detailed literature. The review of the theoretical foundation focus on the development of an ISP. Shirley (2002) indicated that one of the purposes of theory analysis is understanding the existing phenomenon.

3.1.2 Research method

For this research, the researcher used a case study (multiple) method to formulate the research and answer the research question. "It is complete and careful observation of an individual, or an institution is done; efforts are made to study every aspect of the concerning unit in minute details and then from case data generalizations and inferences are drawn" (Kothari, 2004). Policy development projects can be guided by the security development life cycle process (ISPLC), and these procedures include: - The investigation phase: Involve every stakeholder. Next, the analyzing phase: Here, Make a new or recent risk assessment or IT audit. Third step is the design phase: Prepare a plan for how policies should be constructed followed by the implementation phase: The policies must be enforceable as written documents and distributed, read, complied with by those to whom it applies and finally the maintenance phase: Monitor and maintain changes to the policy as needed to ensure that it continues to be effective. Figure 5 illustrates this point.

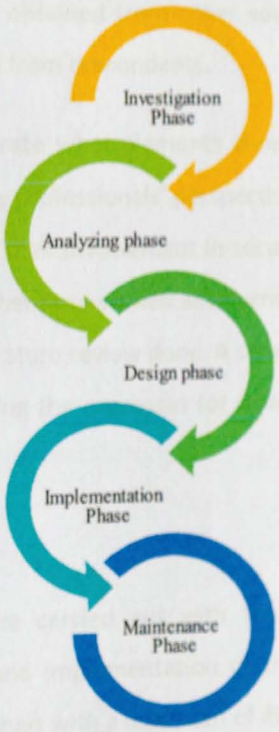

Figure 5. ISPLC

3.1.2 Data collection methods

3.1.2.1 Secondary data collection: The document analysis

A document analysis of information security policy documents was conducted using secondary sources to obtain a thorough understanding of the processes necessary to formulate the policy. These documents constitute institutional documents related to the subject matter. This helped identify the contents of the organization policy document.

3.1.2.2 Primary data collection: The interview

This paper's primary data collection was through an interview, which the researcher has conducted to identify the essential elements of the ISP. According to Kothari (2004), interviews are the most suitable data collection tools for qualitative research and allow for the triangulation of information obtained from other sources. This approach also attempted to get an in-depth opinion from respondents.

The interview is conducted to generate what elements should be included or added in the formulation process from the security professionals' perspective. The respondents were chosen purposefully (purposeful sample) for their involvement in security-related matters in their daily activities and experiences and were therefore viewed as information-rich. The interview is based on primarily on the results of the literature review done. A semi-structured interview questioner was prepared to gather data regarding the processes for developing and implementing an ISP that they felt was necessary.

3.1.2.2.1 Respondents

The semi-structured interviews were carried out with the key personnel responsible for information security development and implementation of the selected banks. IT managers, technical staff, and security professionals with a minimum of five years of experience with IS and ISP development and implementation projects were selected for this study since they would be knowledgeable informants. In order to keep the privacy of the respondent's organizations, each respondent was given a code differentiating one another, which is Respondent 1 – Respondent

15, instead of their actual identity and name of the organization. Data collections through interviews were all conducted by speaking to the respondents face to face while also taking audio recording and field notes. The interview has eleven major questions. Appendix A presents the interview protocol used in this study.

3.1.2.2.2 Role of researcher

Before conducting the interview, the researcher has tried to create a safe atmosphere by keeping a distance of at least 1m from each other and used face masks as per the Ministry of Health guidelines (FMOH) to decrease the spread of the Corona (COVID 19) virus.

According to Lincoln & Guba (1985), to minimize personal bias and increase credibility, validity, and transferability, it is crucial to use member checks during and after the interviews. The researcher reiterated and summarized information, questioning respondents on the accuracy of the information they have given.

Creswell (1994) states that one way to build a great harmony with respondents is to introduce oneself and demonstrate familiarity with the topic. The researcher identified himself as a master's student at Addis Ababa University (AAU). First, respondents were reminded of the purpose of the study, expected benefits, their right to withdraw from the study at any time, and protection of confidentiality. With the respondent's approval, the interviews were audio-recorded to ensure a complete transcript. Written notes were taken during all interviews, enabling the researcher to track key points for use during data analysis.

Respondents were given the interview protocol (Appendix A) a week before their scheduled interview to have time to think about and prepare their responses to the initial questions.

3.1.3 Research area and population

3.1.3.1 Population

The population of the study is twenty (20) banks in Ethiopia, according to the National Bank of Ethiopia (NBE). Sampling techniques were used to select sample banks. Stratified sampling to differentiate the public and private banks since they are homogenous and select sample banks from each stratum. In stratified sampling, it may also be appropriate to choose non-equal sample sizes from each stratum. The proportion for selection was determined by computing the required sample (n) ratio to the study population (N), proportion 5/20=1/4. The stratified bank was multiplied by the obtained proportion to get the number of banks included in the study sample. Five banks were selected for the study from the total number of Banks found in Addis Ababa city Administration after applying the lottery method to select sample banks after stratified sampling.

3.1.3.2 Sample

Sampling is a process of choosing a smaller, more manageable number of people to participate in the research. For most researchers, unless having a considerable budget, limitless timescale, and extensive team of interviewers, it will not be easy to contact every person within the research population (Dawson, 2002). Purposive sampling is appropriate as it matches the expert availability on specifically selected areas. The IS professionals targeted by the survey include IT managers and security professionals. These professionals employed in each bank are small in numbers so the researcher has decided to interview all available. Experienced IT managers from five different banks were selected to understand IS's practice and verify compliance with ISP. Interviewing relevant managers provided a clear picture of the business, reproducible results, and consistency. The respondents were chosen because they are involved in IS-related issues in their daily activities and, therefore, may exert significant influence on IS management in their organizations.

3.2 Research methodology

3.2.1 Data analysis strategy

A thematic analysis method is used in this research for analyzing the data. "It is usually applied to a set of texts, such as interview transcripts"(Srivastava & Thomson, 2015). The researcher closely examines the data to identify common themes – topics, ideas, and patterns of meaning that come up repeatedly. This approach to qualitative data analysis allowed the researcher to set the themes and categories at the start of the analysis. However, this approach also allows for themes and categories that may emerge during data analysis "which the researcher had not stated at the beginning of the study" (Srivastava and Thomson 2015).

The researcher took audio recordings and field notes of the interview sessions. The audio recordings were carefully transcribed verbatim in a Microsoft Word document by the researcher. Field notes were jotted down during each interview and later analyzed and compared to the interview transcriptions. They are used as a supporting data source for this study. On the first page of each set of notes, the researcher recorded the date, time, and title that indicated the content of the notes. Topics addressed in the field notes included the researcher's speculations about emerging themes and particular events that respondents recalled. Other topics included in the field notes direct quotes that caught the attention of the researcher. The researcher immediately highlighted it and put it in the quotation to be easily found during data analysis.

First, after conducting interviews, these transcripts were subsequently imported into the QDA lite software package. QDA Miner is a quantitative and qualitative (mixed methods) data analysis software. QDA miner was mainly designed to assist researchers in managing, coding, and analyzing qualitative data. It is a widely used software for qualitative research. It is used by market researchers, survey companies, government, education researchers, crime and fraud detection experts, and journalists (provalisresearch.com). Figure 6 shows the stages in the analysis of qualitative data. It usually begins with

familiarization of the data, transcription, organization, coding, analysis (grounded theory or framework analysis), and reporting (though the order may vary) (Lacey and Luff, 2001).

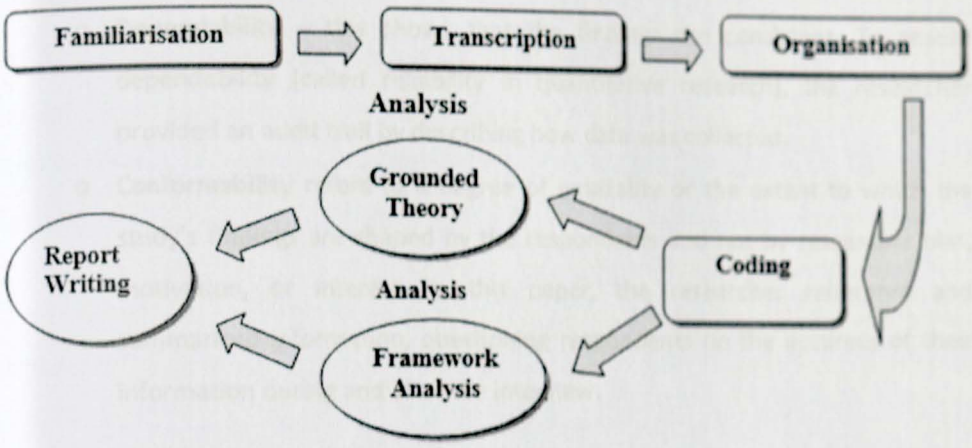

Figure 6. Analysis of qualitative data

Source: Lacey and Luff, (2001).

Next, initial coding was done to find patterns in the data. Following initial coding, codes were compared and combined to create preliminary themes and subthemes. After initial themes were developed, codes within each theme were reviewed to ensure they were consistent with the theme, and modifications were made when necessary. Finally, the themes were reviewed to ensure they represented the data from the interview sessions.

3.2.2 Trustworthiness

Lincoln and Guba (1985) propose four criteria for trustworthiness:-

- **Credibility** – this refers to confidence in the "truth" of the findings. This study is insured by triangulating data.

- **Transferability**– this describes that the findings have applicability in other contexts. The proposed ISP framework provides guidelines that organizations can follow to improve their information security policy mechanisms.
- **Dependability** – this shows that the findings are consistent. To ensure dependability (called reliability in quantitative research), the researcher provided an audit trail by describing how data was collected.
- **Conformability** refers to a degree of neutrality or the extent to which the study's findings are shaped by the respondents and not by researcher bias, motivation, or interest. In this paper, the researcher reiterated and summarized information, questioning respondents on the accuracy of their information during and after the interview.

3.3 Ethical consideration

A support letter written from the university to do the study is used to contact the selected organizations' administration. The data collected from the respondents is used for this study only. In order to validate this research ethically, some components have been considered (Callahan & Hobbs, 1998).

- ✓ Disclosure: respondents have been told about this research's aim and the procedures that have been used.
- ✓ Understanding: make sure that all respondents understand all the information that has been given to them, and they could also ask questions
- ✓ Voluntariness: to participate in the research has been voluntary
- ✓ Consent: respondents have all agreed to participate.

Chapter Four

Data Presentation, Analysis, and Discussion

This is the data presentation, analysis, and discussion part. It tried to present the data collected from banks, discuss the research question, and present the research outcome. In this chapter, the raw data collected through interviews are organized, tallied, and structured to manage presentation and analysis. The researcher's observations are presented through the narrative description. The interview has eleven major questions. Furthermore, hence all the findings presented below are summarized from these eleven interview questions. Additionally, the themes and distribution of codes are presented in table format.

4.1 Demographics of respondents

The findings of this study are based on interviews of fifteen respondents including IT managers, security professionals, and technical staff from five different banks. All the respondents voluntarily participated in the study. They all have adequate experience in IS and ISP development and implementation projects with a minimum of five years of experience. Five respondents had an MSc degree, and ten had a bachelor's degree. Out of the fifteen respondents three were females. All interviews were conducted in April in Addis Ababa, Ethiopia. The frequency distribution of the demographic data are presented in the table below.

Table 4. Frequency distribution of demographic data

CASE	FILE	LOCATION	DEPARTMENT	JOBROLE	EXPERIANCE	SEX	EDUCATION
1	Respondent 1	Bank 1	IT	Manager-IT	>5 years	1 male	Msc
2	Respondent 2	Bank 1	IT	S.officer	>5 years	1 male	Bcs
3	Respondent 3	Bank 1	Operations	compliance offi	>5 years	2 Female	Bsc
4	Respondent 4	Bank 2	IT	IT Manager	>5 years	1 male	Msc
5	Respondent 5	Bank 2	Operations	Divison ma	>5 years	1 male	Msc
6	Respondent 6	Bank 2	IT	Sec. officer	>5 years	1 male	Bsc
7	Respondent 7	Bank 3	IS DPT	DPT head	>5 years	1 male	Bcs
8	Respondent 8	Bank 3	IS DPT	Sec. officer	>5 years	1 male	Bsc
9	Respondent 9	Bank 3	IS DPT	Sec. officer	>5 years	1 male	Bsc
10	Respondent 10	Bank 4	IS DPT	Section head	>10 years	1 male	Bsc
11	Respondent 11	Bank 4	IS DPT	Sec. officer	>5 years	2 Female	Bsc
12	Respondent 12	Bank 4	IS DPT	Sec. officer	>5 years	1 male	Bsc
13	Respondent 13	Bank 5	Operation	Manager	>10 years	2 Female	Msc
14	Respondent 14	Bank 5	IT	Compliance offi	>5 years	1 male	Bsc
15	Respondent 15	Bank 5	IT	Sec officer/Net	>5 years	1 male	Msc

4.2 Research findings

The study produced TEN (10) major themes. These are:-

Theme 1. **Management of security** Theme 2. **Acceptable use** Theme 3. **Data classification level** Theme 4. **Physical and environmental security** Theme 5. **Intellectual property right** Theme 6. **Protection from malicious software** Theme 7. **Continuity of operations** Theme 8. **Information asset management** Theme 9. **Contracts of employment and services** and Theme 10 **Access control**.

Question 1; *How would you describe the different types of information/data you work with?*

Produced **theme 3**.

Question 2; *what are important resources such as customer database, network, etc., that must be protected from a security threat to maintaining the business to operate smoothly?*

Produced **theme 8**.

Question 3; *what are the common security threats in your organization?* Produced **theme 6.**

Question 4; *what prevention mechanisms your organization use?* Produced **theme 4 and theme 10.**

Question 5; *is there information security in your organization? If yes, are you aware about the information security policy content?* And **Question 10**; *what are the advantages of the documents written in your organization that explain the information security policies?* Produced **theme 1.**

Question 6; *How have these policies been developed?* Produced **theme 5.**

Question 7; *How easy to follow are these policies for users?* And **Question 8**; *How are users made aware of the existence and the importance of these policies?* Produced **theme 2.**

Question 9; *what are the most important issues of information security and acceptable use of network systems and information resources in your organization?* Produced **theme 7.** **Question 11**; *what are the most important aspects that require further development in these information security policy documents? Any other comments you want to suggest?* Produced **theme 9.**

Below all the themes with the corresponding codes are presented in the below horizontal bar chart form.

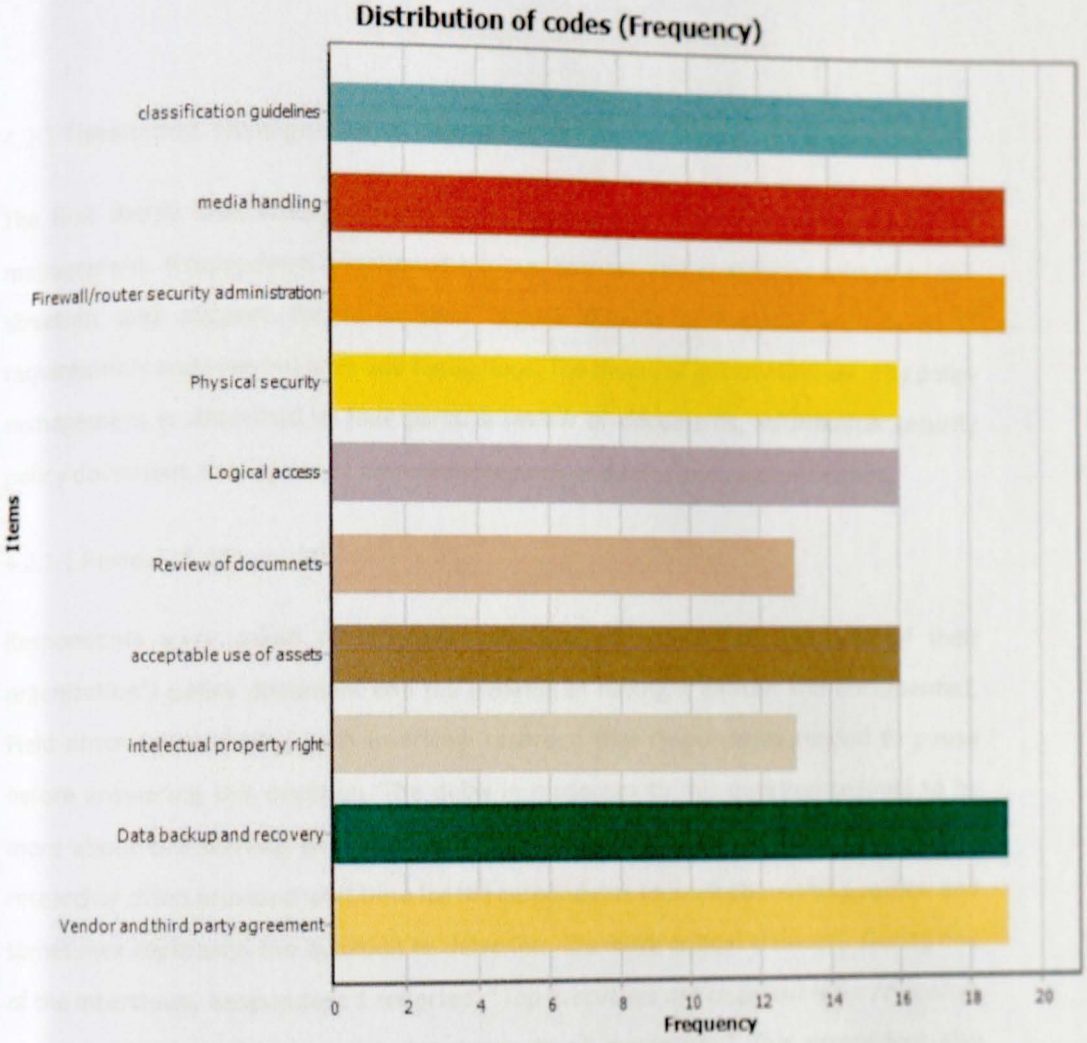

Figure 7. Themes and distribution of codes

Each theme is discussed in further detail below:-

4.2.1 Theme one, Management of security

The first theme that emerged from study respondents' responses pertained to ISP management. Respondents mentioned various barriers and challenges related to the direction and support for IS in their organization in accordance with business requirements and relevant laws and regulations. The theme of information security policy management is described in four parts: a review of documents, information security policy document, management commitment to IS, and roles and responsibilities.

4.2.1.1 Review of documents

Respondents were asked during their interviews to identify the contents of their organization's policy document and the benefits of having it written and documented. Field notes taken during each interview recorded that respondents tended to pause before answering this question. The delay in responses to this question seemed to be more about the starting point of the question than the respondents' responses. The researcher often provided wait time for the respondents to think about this question and sometimes rephrased the question to delve into the more critical elements. During one of the interviews, Respondent 1 reported, "*Top executives are responsible for reviewing, approving and publishing policy documents to all employees.*" This respondent also mentioned that the review frequency must be defined annually at a minimum to ensure its continuing stability, adequacy, and effectiveness.

Respondent 4 went on to say, "*Yes, I know the contents of the policy document. I had once printed it and post on our notice board of the IT department just to create awareness for the staff.*" Another IT manager, Respondent 7, shared a story about that one time he had to review the document because he wanted to know if he can download specific software that is not licensed.

Organizations, most of the time, do not review their documents. Because technological advancements and treats are ever-changing/growing, companies and their corresponding management team should describe the security policy review and approval process.

Respondent 13 said, "*I was able to talk with businesspeople and legislators with my previous employers, and [they] explained to me the advantages of reviewing these documents I never thought of.*"

Respondents 7 and 10 seemed to strongly reflect on this topic and its impact on the company. If significant changes occur and nothing is done, then it will be difficult to ensure its continuing suitability.

4.2.1.2 Information security policy document

The other repeatedly mentioned topic has a well-developed policy document. Respondent 4 provided details, saying: "*Yes, information security policies provide the framework from which all types of users learn the proper procedures in using computing devices and accessing data. Management support is crucial to ensure the security policies are understood and enforced. User awareness and training are provided to users to make them aware of the threats and current trends. It would have been almost impossible without the policy document.*" Information security policy documents seemed to give some respondents a voice they felt they would not otherwise have had. Respondent 7 reported, "*I mean me; personally, I was clueless before, and I think the ability to refer to the document gives users, staff, and us of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets. So it is easier for me, especially for the position that I am sitting, and so I think it is good to have these good documents.*" Every respondent talked about using policy documents for both office and personal use. Overall, all respondents positively on their experiences when it came to IS and ISP documents. A quote from Respondent 10 seemed to summarize the general perceptions about policy documents: "*I think ISP document is a good thing. I think you can use them in effective ways, especially to reduce the risk of security breaches. I know a lot of times, when I had questions asked, I just refer to them, and I would get back to them with an answer. I think that's an effective way to manage, or at least it was for me.*"

4.2.1.3 Management commitment to IS

All fifteen respondents interviewed in this study reported that management should actively support security within the organization through clear direction and commitment. Participant 1 directly stated, "*I am better able to testify to this because I am a manager, and my intent is to support the goals and principles of information security of the company. I am very committed.*" All respondents mentioned that they are serious about the security of their organizational assets. All of the respondents reported that the continuous security threats made them more committed to securing information. Participant 4 responded about his commitment to IS by saying, "*I am, yeah, because securing information of our customers is very critical to our business.*" Having that management commitment helps maintain information value.

4.2.1.4 Roles and responsibilities

After completing the fifteen interviews, it was noted that all of the respondents reported they act based on the roles and responsibilities. Respondents used the terms "roles" and "responsibilities" interchangeably during the interviews.

When respondents reported understanding roles and responsibilities, it was assumed that they meant they could now define IS more accurately because of their experience under the organization's information security policy. Information security roles and responsibilities include responsibility for creating and distributing security policies and procedures; for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel; for creating and distributing security incident response and escalation procedures; for administering user account and authentication management, and responsibility for monitoring and controlling access to data. Respondent 13 said, "*I personally approve the assignment of specific roles and responsibilities for information security across the IT department.*"
In summary, Participant 4 responded to the interview question about the advantages of the documents that explain the IS policies helped better understand his roles and

responsibilities by saying, "*Definitely. I mean, the security roles and responsibilities of employees are defined and documented. It really just becomes second nature.*"

4.2.2 Theme two, Acceptable use

In addition to mentioning the contents and advantages of ISP documents, respondents also mentioned various constraints and practices that users must agree to for accessing corporate networks or information processing facilities.

In Chapter 2, eight essential themes were identified regarding ISP. One of the themes identified was the acceptable use policy. Setting rules like Dos and Don'ts was perceived to promote acceptable/unacceptable use by all the (15 out of 15) of the respondents interviewed. Managers credited having these rules implemented as a major contributor to their risk reduction methodology.

The majority of the respondents gave credit to the acceptable use of corporate assets for promoting responsibility. "*You had to take care of your workstation. It's really just being responsible; doing your work, exerting extreme caution when opening e-mail attachments received from unknown senders, locking the screen or logging off when the device is unattended, and shutting it down when you need to. Once you do those things, the rest will take care of itself, and you'll be a responsible user*," said Participant 3.

Participant 2 stated, "*I actually felt like users had to step up and be more mature using the internet or accessing the company's network. I mean, some users still just messed around accessing social media networks, but some took it seriously, did not want to damage the computer, and used it for work purposes only.*" Respondents' responses to the interview questions showed that most of them believed that the best way to deliver the importance of security policies is to use simple, easy-to-understand words and provide awareness programs to the users, especially employees accessing sensitive information like customer data.

Participant 3 said: "*Training is usually given for the respective users through awareness so as to clarify the contents of the policies. Besides, policies are updated annually and distributed for each users. This is therefore, the policies are easy, accessible for users.*"

4.2.3 Theme three, Data classification levels

A third theme that emerged from study respondents' responses is data classification. The respondents discussed various ways to ensure that information receives an appropriate level of protection. The theme of data classification level is described below in two parts: classification guidelines and information handling/labeling.

4.2.3.1 Classification guidelines

As seen below, most of the interviewees did describe in detail the type of data and method for classification. Interestingly, at least one respondent noted that not every security professional wants data to be classified. To illustrate this point, Respondent 1 said: All data must be given the same emphasis, the same level of attention—some like it when data are classified into different sections, and others do not. Classifying by the level of importance is not suitable for me; maybe by data type, it is ok. On the contrary, respondents 10 said: "*They are different types of information that I work with. In the banking industry, all our information are sensitive. The data in our CBS is especially sensitive. Because it flows cash. Also we have remittance services like swift service. In swift services we handle international currencies. Also I work with user data that work inside the organization. Another type of information I work is cardholder information which use our debit cards.*"

Respondent 6 also said: Information is classified based on its use, kind, criticality, and sensitivity. The different types of information include public information, sensitive information, and private information, confidential and unclassified information. "*Since I started working in this industry, customer information, Card Holder Data, PAN numbers,*

Full Track Data, CVC, and PIN, keys, financial information or transaction are the most confidential tightly controlled."

4.2.3.2 Information handling/labeling

Respondent 5 elaborated on his thoughts by talking about the positive aspects of having a set of procedures based on the classification scheme adopted by the organization. Its impact on the organization handles information; when the information is public and does not impact the employees or the organization, it is labeled "Public." When it is a type of information associated with losses to the organization, if that information was revealed to unauthorized individuals, it is handled as "sensitive." When information in which information loss would impact the company's fundamental business processes, it is labeled as "critical." Moreover, the information is personal information for use within the company labeled as "private." "Confidential" is given to a piece of information when it is used only within the company.

4.2.4 Theme four, Physical and environmental security

The fourth theme that emerged from study respondents' responses pertained to ISP management. Respondents mentioned the various mechanism their organization used to protect information. This theme has been collected under the broader idea of 'the theme of Physical security and environmental security.'

Respondents were asked the type of mechanism their organization used for protecting the company's information, and they all first talked about state of the art secure areas of their data centers and sensitive areas. The responses to this question were confident and more diverse than those given regarding the previous topics raised. For instance, Participant 12 elaborated about how he believed his organization secure areas by saying: Our organization has always had a sound system. Equipment should be protected from

physical and environmental threats. Protection of equipment is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment storage. Unique controls may be required to protect against physical threats and safeguard supporting facilities, such as the electrical supply and cabling infrastructure standardized testing scores.

Participant 11 said: "*We have alarm systems, locks, surveillance cameras, identification cards, and security guards dedicated to these secure areas. I will get a text message when someone entered a secure area like the data center or if there is a fire or flood. I remember that one time I received an alarm text from the system about flood detection. There was a heavy rain that night, and because our data center was located in the basement of the building, it's faced with this kind of things*." Participant 11 continued: "*I had to rush there and used brooms to wipe out the rainwater. So it is beneficial to have these kinds of mechanisms.*"

Additionally, having these redundant kind controls help to control Critical or sensitive information. Processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference because the organization's reputations depend on it.

4.2.5 Theme five, Intellectual property right

A fifth theme that emerged from study respondents' responses pertained to intellectual property rights. Respondents discussed different regulatory agencies and associated regulations, if any, that apply to the organization's business environment. The theme of regulatory compliance is described below in three parts; identification of applicable legislation, technical compliance checking, and regulatory compliance.

4.2.5.1 Identification of applicable legislation

The overall perceptions of the security professionals interviewed for this study were very disappointing regarding the policy development experiences. When asked how have these policies been developed? Even though there is a formal and comprehensive ISP documents in some banks they all said because there is no local standard policy to follow, it is developed in house or a template that's downloaded from the internet.

Respondent 13 explained no formal and compressive developed ISP document; instead, the bank downloaded fragmented policies and procedures from the internet to protect its information. However, the bank is currently in the initiation to develop and implement a compressive bank-wide security policy. "*But we have a plan to adopt NIST framework in the future. As far as policy development is concerned, first assessment has been made to business operations and the associated risks.*"

Respondents 4 and 7 also stated that there is a formally developed ISP which comprises of different sub topics, it is only formulated by the IT security team, and it is approved and signed by the top management committee. Respondent 10 stated: "*we have a well put and defined security policy. I mean, it basically has what we want nothing more nothing less. We use it every day.*"

4.2.5.2 Technical compliance checking

Respondent 13 elaborated that though we do not have a formally developed policy, we comply with some aspects of the operation. For example, for the remittance services like swift service. We handle international currencies swift users in swift services we have to comply with their standards known as 'SWIFT CSCF Customer Security Control Framework.'

Another respondent, respondent 4, said: "*We are a member bank of Premier switch solutions (P.S.S). They are compliant to PCI DSS. Because they are, we also have to be. Every year we renew our license. Based on the comments they have given, we will try to*

amend and fill the gap. But it's difficult because we don't have a comprehensive policy to follow."

4.2.5.3 Regulatory compliance

The majority of the respondents also mentioned that software products are either open source and counterfeited. Respondent 2 said: *"We use a lot of open-source counterfeited software's. The problem with this is that we don't know what's running behind the system. And also it's not reliable."* Respondent 4 also said: appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of proprietary software products. He shared a story by saying: *"One time, during the renewal phase of our PCI DSS compliance, the evaluator (this are third party evaluators that investigate and assess the current status notify PCI), so in that moment he wanted to access on of the user's PC to check if a genuine OS is loaded and has an anti-virus and anti-malware software implemented. Because we do not have a genuine OS system on all our users, we had to change that users PC name to another that has these requirements and give him access. The whole process is on line, so if it was in person, we would have not been compliant."*

4.2.6 Theme six, Protection from malicious software

A sixth theme that emerged from study respondents' responses pertained to protection from malicious software. Respondents mentioned different procedures to ensure the protection of information in networks and protect the supporting infrastructure. The theme of information system integrity and monitoring are described below in three parts: firewall/router security administration, network security and monitoring, and encryption.

4.2.6.1 Firewall/router security administration

Respondents show little confusion when asked to identify the common security threats they face every day. Respondent 12 reported: *"Oh, our security threats are insider threats*

most of the time it's unintentional." Other respondents also mentioned this exact scenario.

Multiple respondents (2, 3, 5, 8, 9, 11, 12, 14, and 15) discussed a particular and common threat: phishing. *"They send you an e-mail which has an attachment, so when you open they will have a full control of your files and ask you for ransom,"* respondent 15 said. Respondent 9 said that when the user is accessing or trying to access unauthorized sites, the firewall will block it. The router/firewall is configured in the network layer to block any unknown source site. Respondent 14 talked about this in detail. He said: *"We actually have implemented Forti-Gate next-gen firewall to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports and limited inbound internet traffic to Internet protocol (IP) addresses within the DMZ. On top of that we use like the Forti-Gate that protects all the way through the application, including the transport layer. We have web based applications that's why we use it."*

Respondent 14 raised one crucial point. He said: *"We use the latest technology, but the one thing that worries me the most is that we don't have a 100% visibility of our networks so that can be an issue."*

4.2.6.2 Network security and monitoring

Several respondents noted that managing vendor accounts were used for support and maintenance of system components. Respondent 6 said: we have vendors accessing our database, the network, and also other systems. *"I mean, it's important to give access to them (the vendors) because they are the experts, and there is no one that can fix whatever the problem is."*

We have controls in place to safeguard the confidentiality and integrity of sensitive data passing over public networks. Respondent 8 said: *"We have data stored or at rest, data at transit which is accessed data so we make sure it's encrypted and hashed. When in use, users are accessing or calling through application. So all of this must be secured."*

Respondents 14 and 15 mentioned the use of V-LANs for every department. V-LANs for operation departments, IT users, and management. Sensitive systems are given static IPs and use the appropriate level of security. Ports are explicitly given to each user, so it also helps for monitoring.

The respondents recalled experiences and situations in which network visibility is a big issue. Respondents were also quick to note how users and the management team handled the presented visibility issue. Some respondents offered ideas and suggestions to employees and team leaders about minimizing the distractions that it presented.

4.2.6.3 Encryption

Respondents reported using a variety of different software programs for the safety of entities' data/information. Respondents were asked to state the software to mitigate the various threats. Respondent 5 said, "*We use open-source software to encrypt and hash data. This makes sensitive data unreadable. We use a hardware security module (HSM) that does all the necessary cryptography and handles Keys.*"

4.2.7 Theme seven, Continuity of operations

A seventh theme that emerged from study respondents' responses pertained to continuity of operations. Respondents raised the issues that need to be considered regarding IS in their organization, including sound network systems and resources to ensure the business continues. The theme of continuity of operations is described below in three parts: data backup and recovery; disaster recovery (DR) and business continuity plan (BCP); and incident response plan and procedure (IRP).

4.2.7.1 Data backup and recovery

All of the respondents believed that having a procedure to help with backup and restorations is very important. Specifically, respondents noted that all assets should be identified and an inventory of all critical assets drawn up and maintained. Respondent 12 said, "*Taking data as a backup is very important part of the business because in case of any failure to the database you can recover from the backed up data and continue to work*

until the main servers are up and running." All respondents talked about the information they work with are sensitive. All data, network systems, and assets are covered in the policy document. Respondent 4 said: The acceptable use policy to govern the use of our network system and information users. This policy is documented stipulating constraints and practices that a user must agree to access the company's network, internet, and other IT resources. Respondents 5, 9, and 11 gave specific examples of backup and restoration procedures. Respondent 14 mentioned logs or automatically generated alerts are generated that document successful and failed backups. He continued by stating, "*we don't have a secure off-site storage of backup media right now, but in the there is a plan to move the DR site to another location, maybe like a district office, something like that*."

Respondent 5 experienced and reported a similar situation. "*Encryption employed during backups and it is automatically done. All we have to do is make sure the data is backed up if not we will manually run the batch.*"

4.2.7.2 DR and BCP

Respondent 4 reflected on his experience during one interview and talked about how little attention to this kind of plan. He reported that he frequently did not approve projects on disaster recovery (DR) site development and business continuity plans (BCP) time because of budget, but most importantly, he could not "*believe it can happen*." This respondent also admitted, saying, "*I hated this projects because I thought they were a waste of money and time developing something we are not going to use. But now once I was involved in one project, I can see how vital these are to the organization*." There are defined requirements like contingency plans that must be developed and implemented to maintain or restore operations following an interruption or failure of critical business processes. Respondent 3 continued from this point and discussed that events that can cause interruptions to business processes should be identified, along with the probability impact of such interruptions and their consequences for information security. "*Actually*

risk assessment (RA) must be performed prior to DR/BCP development. The feasibility, cost return on investment must also be taken into consideration when doing RA. Based on the results of the RA, we describe in the DR/BCP the events that can cause interruptions to business processes, along with the probability and impact of such interruptions and their consequences for information security. Like if our core banking system is down due to, say, natural disaster, we need to have a BCP until we are up and running."

4.2.7.3 IRP and procedure

Respondents often reported that, in general, this goes hand in hand with DR and BCP as it is an integral part of IS. All of the respondents noted this in their interviews. Incident response plan (IRP) procedures must be available in the policy document. Respondent 13 said: *"how the organization identifies and responds to suspected or known security incidents like hacking or phishing and documents security incidents and their outcomes is very important. If the company web site is hacked, we need to identify its point of entry and correct our configurations"*. Respondent 10 also noted the importance of defining procedures that specify when and by whom authorities (e.g., law enforcement) should be contacted after an information security incident if suspected laws may have been broken. *"Collecting and presenting evidence for the purposes of disciplinary action will help us specifically identify the process for modifying and evolving the incident response plan according to lessons learned and incorporating industry developments."*

4.2.8 Theme eight, Information asset management

The eight themes that emerged from study respondents' responses pertained to information asset management. Critical or sensitive information processing facilities should be protected, protected by defined security perimeters, with appropriate policy and procedures. This theme is further discussed in two parts; media handling and asset and capacity management.

4.2.8.1 Media handling

Respondents were asked during their interviews if they were able to identify critical resources that must be protected from security treat. Respondents' responses to the interview questions showed that most of them believed that there is no one specific thing that all organization assets must be protected from any security threat. Respondent 3 said: "*I can mention different resources like network systems...but the most important information resource is the CBS*." Most of them also noted that CBS is the most critical resource to protect. All respondents mentioned that all types of media such as tapes, disks, USB drives, Tablets must be "sanitize" only be used if needed. Respondent 6 said: "*For example, suppose there is debate about whether users should have access to removable media such as USB storage devices. As a security professional, I may believe that such access should never be required, while others may believe it is important to move around data. So the best way to handle this is to define the controls in place to protect media that are transported between sites*".

4.2.8.2 Asset and capacity management

All of the fifteen respondents mentioned the first thing to do in protecting the organization's assets. They believe all assets should be accounted for and have a nominated owner.

Respondent 7 noted that "*Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of the assets. I personally make sure network and informational assets through logs are included an IT asset inventory and the IT asset inventories are performed at least annually*". Respondent 1, who is currently moving to a new location, reported, "*I actually took four or five meetings with my team to identify how resources are monitored and tuned and projections made of future capacity requirements, to ensure the availability and efficiency of systems.*" During these meetings, respondent 1 and his team made future capacity requirements that should be made to reduce the risk of system overload.

4.2.9 Theme nine, Contracts of employment and service acquisition

The ninth theme that emerged from study respondents' responses pertained to contracts of employment and service acquisition. This theme is compromised of the respondents' ideas they deemed necessary and need to be included in the policy document. This theme is put into three separate parts; vendor and third-party management system interconnections and E-commerce.

4.2.9.1 Vendor and third-party agreement

Participants often reported that, in general, they felt that they had to mention these elements because there is a clear consensus about how to handle vendors and third parties. All respondents believe the security of the organization's information and information processing facilities should not be reduced by introducing external party products or services. Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled. Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Respondent 1 mentions that controls should be agreed upon and defined in an agreement with the external party. He said: "*lack of trained workforce to solve issues is the reason to have these kinds of drafts and agreements.*" Thirteen out of the fifteen respondents noted this in their interviews. Participant 4 said: "*I mean, you know there are no set requirements that must be fulfilled before granting a vendor or customer access to the organization's information or assets. If there is a problem with the system or the vendor needs to upgrade the system, he asks to access remote access via Skype or Gmail; we will provide him with a user name and a password. The only thing we check is if it worked or not.*"

4.2.9.2 System interconnections

The other topic that all respondents mentioned that was in line with third party agreement is the documentation process during an exchange of information. "*Once you define those things, the rest will take care of itself, and you'll be ready,*" said Participant

4; formal exchange of communications should be in place to protect the exchange of information through the use of all types of communication facilities. Participant 1 stated, *"I actually use company e-mail to exchange information of the company. I mean some users still just use personal e-mails, but it's important to communicate to 3rd party vendor through secure mediums."* Respondents stated that there is an agreement with the vendors which both parties have signed. *"So if some disagreement pops up we just look at the agreement and follow that in order to exchange data or solve an issue."*

Most of them also noted that a draft of an interconnection service agreement for exchanging information between the organization and external parties should be developed. Some even felt that information involved in electronic messaging should be appropriately protected and controlled.

4.2.9.3 E-commerce

As all the respondents who participated worked at a financial institution, they all had something to say about electronic commerce (E-commerce) as it is always a medium that connects them to different customers through online transactions. However, ecommerce here is described as connections only to the bank and customer or vice versa to pay for services using various applications; mobile, internet, or USSD. The information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. As respondent 10 noted: *"we have different platforms our customers use to pay for services. In this process, the customer is authenticated via his personal identification number (PIN)"*. Respondents explained the different platforms their customers used.

Participant 5 said, *"We customers use USSD or mobile banking, they login via their user name and password, and if they take too long to process the request or somehow the system takes too long it will automatically time out. This helps if a customer is logged in and forgot to complete the payment so other won't tamper with it."*

4.2.10 Theme ten, Access control

In this final section, respondents' responses regarding the prevention mechanism that their organization uses. This theme is produced from the same question that the physical and environmental theme emerged, but here we discuss the logical aspect of the prevention mechanism. The objective of this part is to control access to information. This theme is described into two parts logical access and password management.

4.2.10.1 Logical access

Respondents were asked if they knew besides the physical controls that they rate highly to control the flow of information. Respondent 2 said: when an employee or a user transfers to a new position with different job responsibilities, we modify a user's access rights—for example, when he or she is given more areas to access, like a back end of a database.

Respondent 4 said: The user registration and deregistration procedure (provisioning and revocation) for granting access to information systems are described and defined. *"I personally know that because we have data and internet lines separately. Only privileged users have access to the internet, especially on branches. Only the branch manager has access to the internet all the other user use only data line."*

Respondent 14 also added to this point by stating: *"Different departments have different V-LAN. For swift users we have multi factor authentication which is user name and password plus a token which the system gives."*

4.2.10.2 Password management

The secondary data analysis of this study was a review of the policy documents of the organization. The respondent 7 policy documents show that the password management topics are scattered all over the document. When asked about this, he replied: *"Well, the password controls are in place for operating systems and access to critical applications. Typical password control parameters like complexity and minimum password length are specified but does not have a focal point of reference."*

Respondent 8 talked about how his improved use of solid authentication helped prepare him when accessing secure sites saying, "*I guess making a habit of using a strong password makes feel more secure when handling sensitive data. I think it really kind of helped when access these secure sites and applications.*" Respondent 3 also said: It is essential that all passwords, especially those that are used to access sensitive areas root database passwords, must be rendered unreadable during transmission and storage on all system components, using strong cryptography.

All Respondents all said their system demands the users' password must be complex enough and is frequently changed as per the given time it has been configured.

4.3 Implications and discussions

The study has explored the formulation and implementation of ISP within a five large financial institutions to identify the core values of IS and ISP currently in use. As we can see from the above responses from the case institutions, in general specking, surveyed banks are weak in designing and implementing security policies & procedures. All surveyed banks employed the combination of two or more sources such as: general knowledge and experience of experts, ISO standards, and the internet. They have agreed on the need of a holistic approach in the development process is required. In the process ten major core themes were identified i.e. Management of security, acceptable use, data classification level, physical/environmental, intellectual property right, protection from malicious software, continuity of operations, information asset management, contracts of employment and services, and Access control.

Summary of the findings is as follows;

- Ultimate responsibility for information security rests with the top level management of the organization, but on a day-to-day basis the Network

Administrator shall be responsible for managing and implementing the policy and related procedures.

- Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:
  - ✓ The information security policies applicable in their work areas
  - ✓ Their personal responsibilities for information security
  - ✓ How to access advice on information security matters
- Not all staff comply with information security procedures including the maintenance of data confidentiality and data integrity.
- The Information Security Policy is not maintained, reviewed and updated by the operations group, no time table is defined.
- Line managers are individually responsible for the security of their physical environments where information is processed or stored.
- Each member of staff is not responsible for the operational security of the information systems they use. This is only designated to line managers.
- Each system user don't comply with the security requirements that are currently in force, and do not ensure the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Contracts with external contractors that allow access to the organization's information systems is not reviewed before access is allowed.

Overall, the findings shows that the information security development and implementation level of the researched organizations is unsatisfactory. In the next chapter, the proposed framework is discussed.

CHAPTER FIVE

PROPOSED INFORMATION SECURITY POLICY FRAMEWORK

The chapter presents the proposed entry-level information security policy framework for the Ethiopian banking industry based on the findings of analysis of the research and reviewing existing security governance frameworks.

5.1 Proposed Information Security policy framework-ISPF

Many policies are written to comply with a particular regulation or standard. What should be obvious, but is often overlooked, is that what is stated in a policy should accurately reflect what is happening in the organization's environment (PCI Security Standards Council, 2014). For example, if the policy states a requirement to review firewall and router rule sets at least every six months to comply with the PCI Data Security Standard, the organization must demonstrate that such reviews are taking place. Otherwise, the policy means little because the auditor will note that the organization is "not compliant" with that requirement if no documentation of such a review exists.

Based on literature review, interview findings plus the researchers own experience show that there is no local ISP framework based on the technological advancement of our banking industry that guide the formulation and implementation process of information security. Existing security governance frameworks are contextual and are not customized for Ethiopia. Contextual factors such as organizational, national and environmental affect the design of such documents. There is also a local research gap in this area.

Therefore, based on insights gained from the review of literature on various frameworks such as ISO/IEC27k series, COBIT, PCI DSS,...etc., data analysis of interviews findings, and the student researcher own professional experience an entry level ISPF has been proposed. The proposed framework has ten major themes namely Management of security, acceptable use, data classification level, physical/environmental, intellectual property

right, protection from malicious software, continuity of operations, information asset management, contracts of employment and services, and access control.

5.1.1 Management of Security

- At board level, responsibility for Information Security shall reside with the top level Managements.
- The Network Administrator should be responsible for implementing, monitoring, documenting and communicating security requirements for the organization.

5.1.2 Acceptable use

- An audit trail of system access and data use by staff should be maintained and reviewed on a regular basis.
- The company should have in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy.

5.1.3 Classification levels

All Information in an organization should be classified into one of the four levels based on its sensitivity and the risks associated with disclosure. The classification determines the security protections that must be used for the information. The presumption is that Information will remain at its classification level, as described below. The classification levels are:

- **Restricted** - Information in which its loss would impact the company's fundamental business processes if disclosed.
    - ✓ Personally identifiable financial number (PIN)
    - ✓ Customer information
    - ✓ Passwords or keys
- **Confidential** - Information that could cause risk of material harm to individuals or organization if disclosed. Information that falls outside the restricted

classification but is not intended to be shared freely within or outside the organization due to its sensitive nature and/or contractual or legal obligations.

- ✓ Source code and code reviews,
- ✓ Test results and Intellectual property
- ✓ Contracts, statements of work and/or customer quotations, proposals
- ✓ Management meeting notes

- **Internal** - is given to a piece of information when it is used only within the company.
  - ✓ Draft documents
  - ✓ Meeting notes
  - ✓ End year presentation
  - ✓ Pictures of events, unless specifically taken for marketing purposes
  - ✓ Company social media platforms
- **Public** – Information that's open to the public and does not impact the employees or the organization.
  - ✓ Blogs, social media, whitepapers
  - ✓ Public research documents
  - ✓ Conference presentations given by organization employees
  - ✓ Marketing materials

1.4 Physical/environmental security

- In order to minimize loss of, or damage to, all assets, equipment should be physically protected from threats and environmental hazards.

1.5 Intellectual property right

- The organization should ensure that all information products are properly licensed and approved by the Information Security Officer.

- Users should not install software on the organizations property without permission from the Information Security Officer. Breaching this requirement may be subjected to disciplinary action.

5.1.6 Protection from malicious software

- The organization should use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to cooperate fully with this policy.
- Users should not install software on the organization's property without permission from the IT manager. Users breaching this requirement may be subject to disciplinary action.

5.1.7 Continuity of operations

- The organization should ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

5.1.8 Information asset management

- Each IT asset, (hardware, software, application or data) should have a named custodian who shall be responsible for the information security of that asset.

5.1.9 Contracts of employment and services

- Staff security requirements should be addressed at the recruitment stage and all contracts of employment should contain a confidentiality clause.
- Information security expectations of staff should be included within appropriate job definitions.

5.1.10 Access control

- Only authorized personnel who have a justified and approved business need should be given access to restricted areas containing information systems or stored data.

5.2 Responsibilities for ISPF

The ultimate responsibility for information security rests with the top level management of the organization, but on a day-to-day basis the Information Security Officer shall be responsible for managing and implementing the policy and related procedures.

These top level managers are responsible for ensuring that their employees and contractors are aware of:-

- The ISP's applicable in their work areas
- Their personal responsibilities for IS
- How to access advice on information security matters
- Top level managers are individually responsible for the security of their physical environments where information is processed or stored.
- Each member of employees shall be responsible for the operational security of the information systems they use.
- Each system user should comply with the security requirements that are currently in force, and should also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Contracts with external contractors that allow access to the organizations information systems should be in operation before access is allowed. These contracts should ensure that the employees or subcontractors of the external organization should comply with all appropriate security policies.

The security officer should be responsible for the organizations Privacy Program including but not limited to daily operations of the program, development, implementation, and maintenance of policies and procedures, monitoring program compliance, investigation

and tracking of incidents and breaches and insuring patients' rights in compliance with federal and state laws.

As it was discussed in chapter two on various frameworks such as ISO/IEC27k series documents have major 'say' on these topics. Hence, as shown in Appendix B the major themes are associated with their objectives.

5.3 Evaluation of ISPF

Evaluation method of any given framework vary from one researcher to another. Some of them refine the proposed framework on the basis of suggestions made by the professionals (experts) who were surveyed and collect valid comments; and some prefer evaluate by preparing a workshop for some group of domain experts.

The intent was to locate an IT manager or security professional who has worked on the policy development and implementation projects. However, because respondents were more challenging to find and time constraints ingrained in top management, it did not pan out as the researcher anticipated.

An alternative evaluation method here would be by triangulation. The student researcher has tried to re-code based on the respondent's answers with one another. This provided consistency and reproducible result. On top of that the researcher prepared a 'demo' to one IT expert and collected valid comments. Some of the comments were stated under:-

- The literature review is up to date and comprehensive and clearly identified the gap.
- The sample and the size is clearly stated so that the reader can examine if its representativeness.

- Because the data is collected from 'information rich respondents', all the themes are found and consistent within respondents and across different banks it's safe to say it's applicable but needs to be refined again and again.
- The general and specific objectives are met and the findings support the conclusions. Recommendations are also stated.

Chapter SIX

Conclusion, Recommendations, and Future Works

The last chapter is about the conclusions, recommendations, and future works of the study.

5.1 Conclusion

Today's organizations rely heavily on information and IT. Operational necessity mandates the majority of actions taken by an IT department. Policies are developed to help the performance of the technological environment. Though these are some of the reasons for policy development, it is not the only reason. Informational resources must be protected from any attack or misuse. Security is a crucial part of a banking system not just for the mere function of business operations but to stand out from the competition, especially for an organization like banks, as they acquire sensitive data. So ISPs are there to protect organizational data and define management's strategy for securing sensitive data. Thus, management must be actively involved in providing input, review, and approval of all policy documents.

Accordingly, this study aims to identify what elements of these policies should focus on the technological development of the researched banks and formulate an entry-level ISP framework applicable in the Ethiopian banking industry. The study explored international information security governance frameworks and best practices and chose an ISO audit check list along with the researcher's experience to develop the framework.

The researcher employed a qualitative research approach. Both primary data; through interviews and secondary data; through document analysis are collected and used. The student researcher obtained the information needed to write a relevant policy by asking pointed questions concerning specific subjects. More importantly, this methodology can

help the student researcher determine what security issues exist and the weaknesses and vulnerabilities of the organization. A thematic analysis method is used in this research for analyzing the data. To analyze the data QDA MINER lite v2.0.8 tool is used.

Twenty four (24) core elements (codes) under ten (10) master themes; Management of security, acceptable use, data classification level, physical/environmental, intellectual property right, protection from malicious software, continuity of operations, information asset management, contracts of employment and services, and access control are identified. The study findings show that the core elements availability of policy documents varied among the banks are not consistent. An entry-level ISP framework is formulated. The framework will be the basis of the organizations IS program and serve as a guideline for creating an ISP.

While it is advisable even recommended to refer to international security standards, they are inherently generic. So they must be incorporated into the current structure of the target organization with management input to produce a policy outline. Security policies formulated be written based on the distinctiveness of each and every organization.

5.2 Recommendations

Security policy must always reflect actual practice. Otherwise, the instant the policy is published, the organization is not compliant. It is better to stay policy as a minimal set of mandates to which everyone agrees and may comply than possess a vast approach that few will observe. Then the document will function to enforce policy compliance while the controversial issues are parallelly addressed. The other reason is that, where people are aware that there are no exceptions to policy, they will generally be more willing to help get it right up front to make sure that they will be ready to comply going forward. Once a phrase like "exceptions to the present policy could also be made by contacting the chief responsible of...." slips into the policy itself or the program during which it is used, the document becomes completely meaningless. It not represents management

commitment to an Information Security Program but instead communicates suspicion that the policy will not be workable.

In huge organizations, details on policy compliance alternatives may differ considerably. In these cases, it is going to be appropriate to segregate policies by the intended audience. The organization-wide policy then becomes a worldwide policy, including only the smallest common denominator of security mandates. Different sub-organizations may then publish their policies. Such distributed policies are best where the audience of sub-policy documents may be a well-defined subset of the organization. In this case, an equivalent high level of management commitment need not be sought for an update.

For example, ISP may require only information technology head approval as long because it is according to the general security policy and only increases the management commitment to consistent security strategy. In all probability, it would include such directives as "only authorized personnel should be provided access capable of implementing patch configuration changes" and "passwords for generic IDs should be accessed only within the context of authorized change control processes." Another sort of sub-policy may involve people in several departments engaged in some unusual activity that's nevertheless subject to similar security controls, like encrypting email communications.

On the opposite hand, subject-specific policies that apply to all or any users should not cause a new policy to be drafted instead be added as sub-themes within the master policy. For instance, new organization-wide restrictions on internet access need not replace the "Internet Access" policy. Instead, an "Internet Access" section is often added to the worldwide security policy under information system integration and monitoring. Another caveat for the safety professional using the sub-policy approach is to form sub-policies that do not repeat what is within the global policy, and at an equivalent time, are consistent with it. Repetition must be prohibited because it would allow policy documents to urge out of sync as they individually evolve.

The master document does not mean that the associated information protection goals should be far from the knowledge Security Program. It just means that not all security strategies are often documented at the policy level of executive mandate. As the IS Program matures, the policy is often updated, but policy updates should not be necessary to realize incremental security improvements. Additional consensus could also be continuously improved using other sorts of Information Security Program documents. This paper identified ten major elements (see appendix B) that should be used as the base of an organization's IS program to write an information security policy document that incorporates international standards.

5.3 Future work

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

- Enhancing the same research by considering all of the banks in the country
- Evaluating the maturity level of each of the specific elements
- Assess why banks give less emphasis to ISP

References

Akinlolu, A. (2007). "Information and Communication Technology (ICT) in Banking Operations in Nigeria – An Evaluation of Recent Experiences." The University of Obafemi Awolowo.

Alageel, S. M. (2003). Development of an IS Awareness Training Program for the Royal Saudi Naval Forces (RSNF). Thesis work, Naval Postgraduate School, Monterey, California

Amare, B. (2015). Assessment of Insider Threat in Ethiopian Banking Industry. Thesis work, Addis Ababa University, Addis Ababa.

Anand V. Security policy management process within a six sigma framework. J IS 2012; 3:49–58.

Avolio F, Fallin S, Pinzon DS. Producing your network security policy. Watch Guard Technologies; 2007.

Bayuk J. How to write an ISP. Computerworld 2009. <http://www.computerworld.com/article/2525539/security0/how-to-write-an-information-security-policy.html>.

Balcha R., (2013). "State of Cyber Security in Ethiopia." Ethiopian Telecommunications Agency

Bogale M., (2018). "Proposing an IS awareness program for Enat bank in Ethiopia, Thesis work, Addis Ababa University, Addis Ababa.

Chen H, Li W. Understanding organization employees IS omission behavior: an integrated model of social norm and deterrence. 2014. Proceedings of PACIS, Chengdu, China.

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). California: SAGE Publications, Inc.

Dawson, C. (2002). Practical Research Methods. Oxford, United Kingdom: How To Books Ltd.

Diver S. ISP: a development guide for large and small companies. <http://www.sans.org>; 2007

Doughty K, Grieco F. IT governance: pass or fail? Inf Syst Audit Control Assoc 2005; 6(12):124–32.

Gebrehawariat, D. (2017). Assessment of The Effectiveness of Information Security Management in The Ethiopian Financial Sector: Card Banking Security in Focus. Thesis work, Addis Ababa University, Addis Ababa.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

Hong K, Chi Y, Chao L. An empirical study of ISP on IS elevation in Taiwan. Inf Manag Comput Secur 2006; 14(2):104–15.

InstantSecurityPolicy. (2008). The IT Security Policy Guide: Why you need one, what it should cover, and how to implement it. North Carolina, North Carolina, USA.

ISO/IEC 27001:2009. "Information technology – Security techniques – IS management systems – Overview and Vocabulary ".https://www.iso.org/OBP/UI/#iso:std:iso-iec:27000:ed-3:v1:en

ISO/IEC. (2013). NEN-ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems -. Switzerland: ISO/IEC.

Johannesson, P., & Perjons, E. (2014). Research Strategies and Methods. An Introduction to Design Science, P 39–73. Doi: 10.1007/978-3-319-10632-8_3

Kothari, C. R. (2004). Research methodology: Methods and techniques (Second Ed.). India: New Age International.

KragBrotby W. (2009) "IS Governance: Guidance for IS Managers" IT Governance Institute (ITGI). The USA. www.itgi.org

Lacey, A. & Luff, D. (2001). Trent focus for research and development in primary health care: An introduction to qualitative analysis. London: Trent Focus.

Latham, R. (2013) Information Management Advice 35: Implementing Information Security. Retrieved November 2013, from: https://www.informationstrategy.tas.gov.au/RecordsManagementPrinciples/Document%20Library%20%20Tools/Advice%2035%20Implementing%20Information%20Security%20Part%204%20-%20IS%20Policy.pdf

Lisa Given, 2008 The SAGE Encyclopedia of Qualitative Research Methods SAGE DOI: http://dx.doi.org/10.4135/9781412963909.n398

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Newbury Park, CA: Sage Publications, Inc.

Mark R.Ousley (2013). "Complete Reference: IS." 2nd edition, McGraw, USA

Michael E. Whitman, Herbert J.Mattord, (2012) "Principles of IS," Kennesaw State University. 4th edition.

McGlasson, L. (2007, October 26). Tjx update: Breach worse than reported. Bank Info Security

McKenna S. keeping it real: updating your security policy. Inf Secur J 2010; 7(2):18–21.

Munirul Ula, Zuraini bt Ismail, and Zailani Mohamed Sidek (2011). A Framework for the Governance of IS in Banking System, Journal of Information Assurance & Cybersecurity, pp.1-12

National Computer Board. Guideline on ISP. <http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Information%20Security%20Policy.pdf>; 2011

National Institute of Standards and Technology (NIST, 2012). Risk assessment framework

Negussie, A. (2015). Practices, Challenges and Prospects of Information Security Policy in Ethiopian Banking Industry. Thesis work, Addis Ababa University, Addis Ababa.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). National Institute of Standards and Technology Special Publication 800-12 Revision 1. Gaithersburg: NIST

NIST. (2003). Building an Information Technology Security Awareness and Training Program. Gaithersburg: U.S. Government Printing Office.

PCI Security Standards Council. (2014). Information Supplement: Best Practices for Implementing a Security Awareness Program. PCI Security Standards Council.

SANS Institute. (2018, May 15). About Us: SANS Institute. Retrieved from SANS Institute Web site: https://www.sans.org/

Roberta Heale and Dorothy (2013). Forbes Understanding triangulation in research Design Theory in Information Systems Article in Australasian Journal of Information Systems •

Shirley Gregor (2002), Design Theory in Information Systems, Article in Australasian Journal of Information Systems• November 2002 DOI: 10.3127/axis.v10i1.439 • Source: OAI

Straub D. (1990), "Effective IS security," Information Systems Research, vol. 1, USA.

Tebkew, K. (2013). IS Management Framework for Banking Industry in Ethiopia. Thesis work, Addis Ababa University, Addis Ababa.

Von Solms R, Thomson KL, Maninjwa M. IS governance control through comprehensive policy architectures. Johannesburg, South Africa: In ISSA; 2011.

Woretaw, A., & Lessa, L. (2012). IS Culture in The Banking Sector in Ethiopia. 5th ICT 2012 Ethiopia Conference (p. 22 pages). Addis Ababa.

Appendix A: Outline of the Interview

Department:

Sex:

Education:

Job Role:

Years of Experience:

1. How would you describe the different types of information/data you work with?
2. What are important resources such as customer databases, networks, etc., that must be protected from a security threat to maintain the business to operate smoothly?
3. What are the common security threats in your organization?
4. What prevention mechanisms your organization use?
5. Is there IS in your organization? If yes, are you aware about the ISP content?
6. How have these policies been developed?
7. How easy to follow are these policies for users?
8. How users are made aware of the existence and the importance of these policies?
9. What are the most important issues of IS and acceptable use of network systems and information resources in your organization?

10. What are the advantages of the documents written in your organization that explain the IS policies?

11. What are the most important aspects that require further development in these ISP documents? Any other comments you want to suggest?

Appendix B: Entry-level Policy and Objectives

Themes	Objective
Management of security • ISP document • Review of ISP • Management commitment to information security • Roles and responsibilities	To provide management direction
	To manage information security within the organization.
	To understand the roles and responsibilities of every stakeholder.
Acceptable use Acceptable use of assets	To achieve and maintain organizational assets.
Data classification levels • Classification guidelines • Information handling	To ensure that information receives an appropriate level of protection.
Intellectual property right • Identification of applicable legislation • Intellectual property right Regulatory compliance	To avoid breaches of any law ensure compliance of systems with organizational security policies and standards

Physical/Environmental security Physical security	To prevent unauthorized physical access.
Access control • Logical access • Password management	To prevent unauthorized access to information systems.
Protection from malicious software • Firewall/router security administration • Network security and administration ? Encryption	To ensure the secure operation of assets and protect information in networks.
Continuity of operations • Data backup and compliance • DR and BCP • IRP and procedure	To maintain the integrity and availability of information and counteract interruptions to business activities and major failures of information systems or disasters.

Information asset management • Media handling • Asset/capacity management	To handle all assets in the organization.
Contracts of employment and services • Vendor and third-party agreement • System interconnections • E-commerce	To maintain the security of the organization's information and facilities that are accessed, or managed by external parties.

Appendix C: Support request letter

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ትምህርት

Addis Ababa University
College of Natural Science
School of Information Science

Date: April 19, 2021
Ref No. SIS/42/2021/13

To Whom It May Concern

Subject:- Student Yoseph Getu

Dear Sir /Madam,

Student Yoseph Getu (ID.No GSR/4352/12) is graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a M.Sc. Thesis research under the title "Formulating a Standard Information Security Policy for Ethiopian Banks".

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

With Regards

Tibebe Beshah (PhD)
Head, School of Information Science

: 1176 Email: information_sci_cns@aau.edu.et : +251-(11)-122-91-91