ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCE
SCHOOL OF INFORMATION SCIENCE

PRACTICES, CHALLENGES AND PROSPECTS OF INFORMATION SECURITY POLICY IN ETHIOPIAN BANKING INDUSTRY

A thesis submitted to College of Natural Science of Addis Ababa University in partial fulfillment of the requirements for the Degree of Master of Science in Information Science

2015

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCE
SCHOOL OF INFORMATION SCIENCE

PRACTICES, CHALLENGES AND PROSPECTS OF INFORMAITON SECUIRTY POLICY IN ETHIOPIAN BANKING INDUSTRY

By

Abeselom Negussie

2015

Name and signature of members of the examining board

Name	**Title**	**Signature**	**Date**
Dr. DerejeTeferi	Advisor,		
Dr. Workshet Lamenew	Examiner,		
Dr. Tibebe Beshah	Examiner,		

DECLARATION

I, the undersigned, declare that this thesis is my original work and has not been presented for a degree in any other university, and that all sources of materials used for the thesis have been duly acknowledged.

_____

Abeselom Negussie

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

_____

DerejeTeferi (PhD.)

Dedication

I would like to dedicate this paper to my late brother Misikir Negussie, who believed in me, who shows me the right direction in life.

Acknowledgement

First and foremost my special thanks go to the almighty God for his forgiveness with the courage and endurance to successfully complete this research work.

It is a pleasure to thank the people who helped me during the whole process of the thesis.

Firstly my thanks go to my advisor Dr. Dereje Teferi for his unlimited supervision, valuable comments and for showing me the right direction for the study.

Then I would like to thank my family members (Negussie Mengesha, Fantaye Haile, Tseday Negussie, AdeyAbeba Negussie) for their support in every aspects of life and their moral support throughout my study. I would also like to thank my friends (Abel, Fasil and Johnson) for their moral support and encouragements throughout the study.

Finally I would like to thank my colleagues (Behailu, Dada, Brook, Ermi and GK) for being there with me throughout the study.

My special thank goes to the school of Information Science for allowing me to conduct the research

Abstract

Information is one of the primary assets of any organization. Thus in today's business environment any organization depends on information and information technology. Information security has become the major concerns and challenges facing any organization.

Ethiopian banking industry is one of the rapidly growing industries in the country with the advancements of information technology. This thesis work assesses how Ethiopian banking industry's information security and information security policy practices is.

This research answers the following research questions: how is the current practice of information security and information security policy in Ethiopian banks? What are the challenges in formulation, implementation and compliance of information security policy in Ethiopian banks? What are the future prospects of Information security policy in Ethiopian banks?

Assessing the practices of information security and identifying the challenges of information security policy helps the banking industry to formulate and implement their information security policies efficiently and effectively. It will also help to inspire researchers on the study area.

For the purpose of the research qualitative type of research is selected. Both primary and secondary data are used. Primary data is collected through interviews and the researcher's observations and secondary data is collected from journal, Internet, published statistical resources, bulletins etc. 11 banks are chosen for the study including National Bank of Ethiopia.

Managements lack of awareness, lack of industry best practices and standards in the country, lack of professional in the area are among the major challenges Ethiopian banks faces.

Table of Contents

List of Tables

List of Figures

List of Acronyms

AIB	Awash International Bank
CBB	Construction and Business Bank
CBE	Commercial Bank of Ethiopia
CIA	Confidentiality, Integrity and Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
COBIT	Control Objectives for Information and Related Technology
DBE	Development Bank of Ethiopia
E-mail	Electronic mail
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standards
ISP	Information Security Policy
IT	Information Technology
LAN	Local Area Network
NBE	National Bank of Ethiopia
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OIB	Oromia International Bank
PCI DSS	Payment Card Industry Security Standards Council
PSS	Premium Switch Solutions

Chapter 1 Introduction

1.1. Background

Today's business environment is in a very dynamic and rapid change due to lots of technological innovation, increased awareness and demands from customers. "The application of information and communication technology concepts, techniques, policies and implementation strategies to banking services has become a subject of fundamental importance and concerns to all banks and indeed a prerequisite for local and global competitiveness" [6].

Now a days the world can no longer function without information technology. Essential infrastructures including transportation system, banking and the financial markets, the entertainment industry, the health care system, government, the military and the education system can no longer survive without modern information technology. This increasing dependence on information technology creates new opportunities for the benefit of society [24]. In other words computer has been widely applied in every aspects of our day to day life from business, government, education, finance, healthcare, and aerospace to defense system. With our increasing dependency on information technology the consequences of computer crime can be extremely serious[3].

Information security has become major concerns and challenges facing organizations [45]. Despite the effort and money that organizations spend to secure their assets, many incidents of data breaches and information loss continue to happen every year. Today, every organization realizes that securing information is a continuous and complex task. The burden of keeping information secure rests on the shoulders of all organizational business units and members[1].

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. But Information Security Management is the process of

protecting electronic and non-electronic information assets against the risks of loss, misuse, damage, and disclosure or corruption [9]. As [27] stated, recognizing the importance of information security to the core business is one of the first steps in building an effective information security culture.

An Information Security Management System is a component of the overall organizational management system. This component uses a business risk approach, in order to establish, implement, monitor, review and maintain controls in order to improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources[5].

The creation of information security program begins with the creation and/or review of the organization's information security policies, standards and practices [15]. Policies shall be considered as the basis for all information security planning, design, and deployment.

A policy is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the organization. Like laws, policies define what is right, what is wrong, what the penalties are for violating policy, and what the appeal process are [5].

Information security policy is mainly determined by an environment in which various information are being used and communicated. The environments, in which different kind of information are used, from the point of view of information criteria of confidentiality, integrity and availability, have been changing a lot throughout the last twenty years [2].

Information security professionals help maintain security through the establishment and enforcement of policies. These policies serves as guidelines which describe acceptable and unacceptable employee behaviors in the workplace which function as organizational laws, complete with penalties, judicial practices, and practices to require compliance. Because these policies function as laws, they must be formulated

and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace [12].

With the increasing effect of technology and globalization, organizations have started to use information technologies in various functions and departments in the last decades [10]. Organizations must treat information as any other resource or asset. It must be organized, managed and disseminated effectively for the information to exhibit quality. Within an organization, information flows in four basic directions as upward, downward, horizontal and outward/inward [7]. Taking into account that there is a huge amount of information flow in organizations, it is necessary to consider how to secure this information.

As [14] stated, "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". Now a day customers are very concerned about privacy and identity theft. Business partners, suppliers, and vendors are seeing security as one of the top requirement. Banks' ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network services [12].Attacks like spyware, Trojan horses, and key loggers, can cause a user to unintentionally download malware developed for the malicious intention of collecting various user information. The stolen information can be used for identity theft, which is a much more insidious prospect than the account skimming or account takeover associated with the more common phishing attacks [12].

In today's technological and social environment, security is a very important part of a banking and financial institution system. Business partners, suppliers, and vendors require high information security from one to another, particularly when providing mutual network and information access [13].With the increasing daily reliance on electronic transactions, it is essential to have reliable security practices for individuals, businesses, and organizations to protect their information.

1.2. Statement of the Problem

Due to technology transformation and national information Security policy in today's Ethiopian banking business, Information security becomes one of the key points for customer attraction, retention, and profitability. Thus, in order to get national and international competitive advantages, information like other assets must be properly managed from its creation up to disposal [4].

Ethiopian banking industry is one of the rapidly growing industries in the country [27]. Even if Ethiopian banks are late to move with the technological advancement, currently they are on the right track to move forward. The banking industry is undergoing fast progress in migrating its major business processes towards IT-based services; one of the technologies that banks are investing in is that e-banking. Provision of e-banking services is considered as one of the competitive advantages [27].As [28] one of the major barriers in the adoption of e-banking in Ethiopia is security risk. So the banking industry has to give big concerns regarding information security, since it has a sensitive data which is the financial transaction.

A computer crime starts, and ends, with a human, no matter which method is chosen for the attack. Many successful computer crimes could have been prevented if the people involved had been alert to information security, conscious of security, or aware of their own weaknesses [13].

To secure information assets and to reduce the risk associated with these systems, organizations typically concentrate on technical and procedural security measures. Although these solutions help improve information security [8], relying on them alone is not enough to eliminate risk. Even though organizations are investing more in technology-based information security solutions, evidence from empirical surveys found that respondents reported large increases in information security incidents [11].

As [15] stated information security issue is not only a problem that technology can address alone but also a problem of a management to solve. Therefore, legal frameworks

in the form of policy and standards are the primary prerequisites to establish efficient and reliable security governance systems.

[27] Assesses the practices of information security culture in Ethiopian banking industry. The researchers found that the level of information security awareness in the banking sector is unsatisfactory.

Information security and data protection have become important concerns and challenges facing banking industry and users, since the banking industry have a very sensitive data. Information security researchers have recently emphasized that management's attention is required to secure information resources to design effective security policies and to enhance users' security awareness to comply with information security policies [13].

Therefore, due to the above facts Information Security Policy must be designed to provide employees with guidelines on how to address the integrity, availability, and confidentiality of information resources they use in performing their jobs. As a result assessing the challenges and prospects of information security policies in the Ethiopian banking industry helps the banking industry. This research's aim is to assess the current practices of information security and ISP and to investigate the challenges and prospects of ISP in Ethiopian banking industry.

This research intends to answer the following research questions:

- How are the current practices of information security in Ethiopian banks?
- What is the status of ISP in the Ethiopian banking industy?
- What are the challenges in formulation, implementation and compliance of ISP in Ethiopian banks?
- What are the future prospects of ISP in Ethiopian banks?

1.3. Objectives of the study

1.3.1. General Objectives

The general objective of this study is to assess information security and ISP practices, and to identify the challenges and prospects of information security policy in the Ethiopian banking industry.

1.3.2. Specific Objectives

To achieve the main goal, the study has the following specific objectives

- Assessing how banks are engaged in current information security practices
- Identifying the problems that impede in formulating ISP
- Identifying the problems that impede in implementing ISP
- To investigate the prospects of ISP
- To propose possible recommendations in formulating and implementing ISP

1.4. Significance of the study

The research helps to identify the challenges and prospects in the process of formulation and implementation of ISPs within the Ethiopian banking industry. Since the research tries to identify the challenges, banks will benefit on doing only to find a solution for these challenges. The study also tries to identify factors that affect the enforcement of ISPs.

The proposed recommendations will let banks to formulate and implement their ISPs efficiently and effectively. And it will also be expected to serve as a baseline to inspire other researchers on this study area.

1.5. Scope and Limitations of the study

The scope of the research is limited to assessing the current information security policies and information security practices; and identifying its main challenges and finally proposes a recommendation for a successful formulation and implementation of information security policy.

The result of the research would be more fruitful if it is conducted widely by including all the banks in Ethiopia. However, due to time, labor and money constraints the study is limited to conduct the practices, challenges and prospects of information security policies in one central bank, three government owned and seven private banks only.

The other major limitation of the study is that it doesn't involve employees/users from different business units due to the preliminary study taken, which finds that users lack of awareness and users are afraid of providing such information due to their thought that giving such information might jeopardize the organizations reputations.

1.6. Organization of the paper

This thesis is structured into five chapters. It has an introductory chapter which includes an introduction, statement of the problem, objectives of the study, the research methodology used for the research, significance of the study and scope and limitations of the study.

Chapter two reviews related literature on the general context of information security and information security policy. It particularly discusses the evolution of information security and ISP, the CIA triad, information security threats, information security awareness, information security governance, purpose of ISP, fundamentals of ISP and common ISP applicable in the world.

Chapter 3 which discusses the methodology used for conducting the research which tries to show what the research design is, the study population and outline of the interview and what the interview questions intends to find.

Chapter 4 is the data presentation, analysis and discussion part. It tries to present the data collected from each bank and finally discusses the research questions and what are the outcomes of the research.

The last chapter which is chapter 5 is about the conclusions, recommendations and future works of the study.

Chapter 2 Literature Review

In this chapter both conceptual literatures and related works are reviewed. In the conceptual literature review; overview of information security, evolution of information security, the CIA triad, information security strategies, information security threats, information security awareness, information security governance and overview of information security policies are discussed.

2.1. Conceptual Literature Review

The purpose of this conceptual literature review is to have an in-depth understanding about information security and Information Security Policy. This sub-topic covers: Overview of Information Security,

Information is an important asset for any organization and as [5] also stated that "The more information we have at our hand, the better we can adapt to the world around us". Among an organizations asset, information is often one of the most important assets. Information differentiates companies and provides leverage that helps one company become more successful than another. As it is an important asset, management is expected to ensure that appropriate levels of control are in place to protect this useful resource.

A successful organization should have the following multiple layers of security in place to protect its operations [18]:

- Physical security: to protect physical items, objects, or areas from unauthorized access and misuse
- Personnel security: to protect the individual or group of individuals who are authorized to access the organization and its operations
- Operations security: to protect the details of a particular operation or series of activities

- Communications security: to protect communications media, technology, and content
- Network security: to protect networking components, connections, and contents
- **Information security**: to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved through the application of policy, education, training and awareness, and technology.

2.1.1. Overview of Information Security

Organizations classify information in different ways in order to differently manage aspects of its handling, such as labeling, distribution, duplication, release, storage, encryption, disposal, and methods of transmission. The specifics are spelled out in an organization's information classification and handling policy, which represents a very important component of an organization's overall security policy[9].

Information security refers to protecting or safeguarding any kind of sensitive information and information systems from unauthorized access, disclosure, modification, disruption and destruction [9]. For most organizations, information is the critical resource to be secured. If sensitive information fails into wrong hands, then the respective organization may face a great deal.

As [5] "Security is a paradigm, a philosophy, and a way of thinking". The best approach to security is to consider every asset in the context of its associated risk and its value, and also to consider the relationships among all assets and risks [5].

According to [46] until recently a major focus of information security has been the protection of the IT systems that process and store the vast majority of information, rather than the information itself. But this approach is technology-centric and too narrow to accomplish the level of integration, process assurance and overall security that is now required.

Information intended for internal use only is usually meant to be seen by employees, contractors, and service providers, but not by the general public. Examples

include internal memos, correspondence, general e-mail and instant message discussions, company announcements, meeting requests, general presentation materials etc. This type of information is typically the least restricted because spending a lot of time and money on protecting it doesn't outweigh the value of the information or the risk of its disclosure [5].

Companies may have confidential information, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts, and earnings announcements, which are intended for internal use on a need-to-know basis. Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement or equivalent obligation of confidentiality [5].

2.1.1.1. The Evolution of Information Security [5, 18, 26]

In the early days of networking, individual computers were connected together only in academic and government environments. Thus, at that time, the networking technologies that were developed were specific to academic and government environments. Originally, the academic security model was "wide open" and the government security model was "closed and locked." There wasn't much in between. The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data, this method of protecting assets provided a hard-to-penetrate perimeter.

In the academic world, the goal was to share information openly, so security controls were limited to accounting functions in order to charge money for the use of computer time. The government model blocks everything, while the academic model allows everything. There is plenty of room in between these two extremes. In the field of computer security, the practices established by the academic and government institutions persisted until the early 1990s, and some of those practices are still around today. Those practices that have endured continue to have their place in a comprehensive security

strategy, but they are no longer sufficient to meet the needs of the modern computer network.

When businesses started to widely embrace the Internet as a sales channel and business stool in the early-to-mid 1990s, a new security model was required. A closed-door approach doesn't work when you need to allow thousands or millions of people to have access to the services on your network. Likewise, an open-door approach doesn't work when you need to protect the privacy of each individual who interacts with the services on your network.

E-commerce and business required a more blended approach of providing limited access to data in a controlled fashion, which is a more sophisticated and complex approach than that used by the earlier security models. Partial controlled access requires authentication, authorization, and privacy and more complexity. As the use of information technologies evolved, the original all-or-nothing approaches to security no longer met the needs of information consumers. So, the practice of network security evolved. The concepts of intranets and extranets were developed to accommodate internal and external customers, respectively, with secured boundaries that resembled miniature versions of the firewall perimeter. Virtual private networks (VPNs) were developed to provide a secure channel (or tunnel) from one network to another.

The history of information security begins during World War II when the first mainframes developed to aid computations for communication code breaking in use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards. During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage.

Throughout the first decade of the 21st century, the Internet continued to become an increasingly critical business platform, and the network became more of a key business

component. As more companies started doing business on the Internet, concepts such as Software-as-a-Service (SaaS) were developed to provide business services over the Internet. And the threats found on the Internet evolved as well. Basic viruses and worms along with the simple exploits and man-in-the-middle attacks found in the decade of the 1990s became more sophisticated, effective, and ubiquitous, which brings us to today. Business partners need to share information with our company, and often with each other as well. Employees, consultants, contractors, service providers, system integrators, and other entities that augment a company's resources all need to collaborate with a pool of information. The better the distribution vehicle for that information, the more business opportunities that can be accessed by the company. Customers require secure access to the information that they need. A secure data network allows a company to distribute information quickly and effectively throughout the organization, to business partners, and to customers.

The threats to information are varied. They are technical, physical, and human in nature. To counter these threats, information security has evolved over the past few decades. We are today, in the third generation (3G) of information security. It has evolved from its initial focus on technology, to its focus on processes (standards, best practices) and to the current focus on the human element that manages or uses the technology and processes.

The shift in focus from technology to processes, and subsequently the human element, has come with the realization that technology and processes are only as good as the human beings that use them.

The evolution of the information security model has occurred due to the evolution of the type of threats that businesses are faced on a day-to-day basis. The threats have evolved and become more sophisticated. Typical threats that occurred during the technology implementation phase were viruses, worms, distributed denial of service (DDOS), and so forth. Use of firewalls, anti-virus, and IPS systems grew as a means of countering those threats. Human element related threats during this phase were device miss-configurations, excessive trust in security technology, and security flaws within the technology itself. The other major problem was security flaws within the technology itself.

For example, security flaws within the software that were installed in firewalls, anti-viruses, and so forth.

Typical threats during the process implementation phases were: too much reliance on documentation and absence of actual practice. This phase does justice to the saying "documented but not practiced." For example, organizations invested time and money in documenting policies, processes for information security, especially during the periods of legal regulations and compliance. The result was that there were numerous documents that helped the organizations to comply to legal regulations but did not substantially reduce information security risk.

The main reason why technology and processes have not managed to effectively bring down the instances of information security incidents is because the people entrusted with managing the technology and processes were not motivated, aware, responsible, and qualified for information security management.

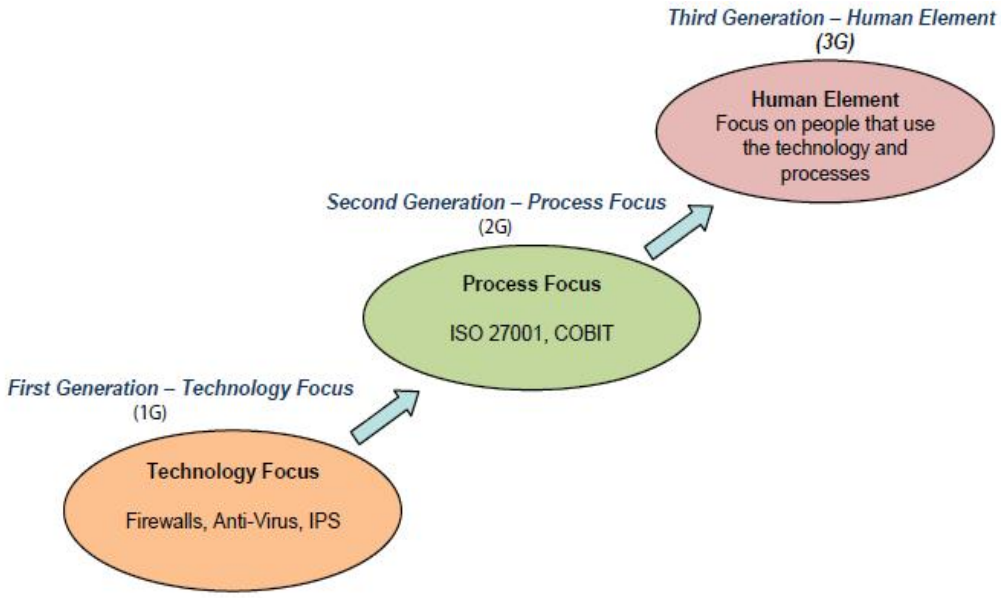

Figure1. Evolution of Information Security [26]

2.1.1.2. The CIA Triad

As many scholars stated that the primary goals and objectives of security are contained within the CIA Triad, in other words all security programs start with the CIA triad [16], which is the name given to the three primary security principles.

- Confidentiality
- Integrity
- Availability

Figure 2. The CIA Triad

Confidentiality

Confidentiality means that the assets of a computing system are accessible only by authorized parties in other words it means that the information that should stay secret stays

secret and only those authorized to access it may receive access. Confidentiality is sometimes called secrecy or privacy. Unauthorized access to confidential information may have devastating consequences in any organizations [18]. Examples of confidentiality threats are malware, intruders, social engineering, insecure network etc.

Integrity

Integrity is concerned with the trustworthiness, origin, completeness and correctness of information as well as the prevention of improper or unauthorized modification of information [18]. In this context, modification includes writing, changing, changing status, deleting, and creating. In information security context integrity not only refers the integrity of the information itself but also to the integrity of source. There are two broad mechanisms for integrity, the preventive and the detective. Preventive mechanisms are like access controls which prevents unauthorized modification of information and Detective mechanisms are intended to detect when preventive mechanisms failed in case of unauthorized modification.

Availability

Availability means that assets are accessible to authorized parties when they need to access. In simple words it is the uptime of computer based services [5]. An authorized party should not be prevented from accessing objects to which he/she, or it has legitimate access needs. For example, a security system could preserve perfect confidentiality by preventing everyone from reading a particular object. However, this system does not meet the requirement of availability for proper access.

Along with the fundamental basis of the CIA triad, a security program must start with the proper policies and must gather input from all the senior leadership of the organization [20].

Other Security Concepts

Identification: is the first step in the identify-authenticate-authorize sequence that is performed everyday activities within an organization. It is a mechanism by which to claim a person. It can be a unique name or unique identity number to identify someone in an organization or on a given system [30].

Authentication: happens just after identification which verifies the authenticity of the identity. In this stage where we can prove that a given person is indeed the person that claims to be. There are three methods of authentication these are what we know, what we have and what we are [18]. What we know is like passwords, passphrases, secret codes and PINs (Personal Identification Numbers). What we have is like keys, USB tokens and smart cards. Lastly what we are refers to biometric authentication methods like finger prints, retinas, voice recognition etc.

Authorization: after proving a user at the authentication stage, users are assigned to a set of rights, privileges or permissions which defines what they can do on the system. Theses authorizations are most commonly defined by the systems security policy and are set by the security administrator [5].

Accountability: refers to the possibility of tracing actions and events back in time to the users, systems or processes that performed them, to establish responsibility for actions or omissions [5]. A system may not be considered as secure if it does not provide accountability, because it would be impossible to ascertain who is responsible and what did or did not happen on the system without that safeguard. Accountability is mainly provided by logs and audit trails [5].

Non-repudiation: refers to one of the properties of cryptographic digital signatures that offers the possibility of proving whether a particular message has been digitally signed by the holder of a particular digital signatures private key. Refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. It is a way of

guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message [18].

It prevents user who are the information source from denying the fact that they have sent information or users from denying the fact that they have received information.

2.1.1.3. Information Security Strategies

The field of security is concerned with protecting assets in general. Information security is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication. Defense, Detection and Deterrence (the three Ds) are the three aspects of security that can be applied as a security strategy within an organization [5].

Defense aims to protect information assets prior to an attack by prohibiting unauthorized asses, modification, destruction or disclosure [21]. It is often the first part of security that comes to our mind. The desire to protect ourselves is instinctive, and defense usually precedes any other protective efforts [5]. Defensive measures reduce the likelihood of a successful compromise of valuable assets, thereby lowering risk and potentially saving the expense of incidents that otherwise might not be avoided. Conversely, the lack of defensive measures leaves valuable assets exposed, inviting higher costs due to damage and loss. Defensive strategies can be used to avoid information leakage, for example a clean desk policy can be useful for misplaced sensitive documents in an organization. Defensive controls on the network can include access control devices such as Stateful firewalls, network access control, spam and malware filtering, web content filtering, and change control processes. These controls provide protection from software vulnerabilities, bugs, attack scripts, ethical and policy violations, accidental data damage, and the like[5]. However, defense is only one part of a complete security strategy.

Detection on the other hand is an operational level strategy which aimed at identifying specific security behavior [22]. According to [5] we have to know about the specific security incident before reacting to the incident. Various security technologies can be applied with in this strategy like network detection devices, network scanners, system

scanners, video surveillance systems, misuse and anomaly detectors, antivirus software etc. [21]. A security breach may go unnoticed for hours, days, or even forever without a proper detection mechanism [5].

Deterrence is another aspect of security which is aimed at in influencing human behavior and attitude in their disciplinary action. It is considered to be an effective method of reducing the frequency of security compromises, and thereby the total loss due to security incidents [5]. It is applied internally which aims at company personnel. It is effective in guiding employees towards legitimate, acceptable use behavior, in discouraging weakly motivated internal perpetrators, in reducing insider abuse and misuse of information systems, and in influencing employee intentions [24]. In other statement deterrent controls are implemented for employees using threats of discipline and termination of violations of policy. One of the main focuses of deterrence is in security policy, where it has been used to specify punishment of employees that fail to adhere to policy statements. Each of the three Ds is equally important, and each complements the others [24].

2.1.1.4. Information Security Threats

With the development of Information and Communication Technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats, which can cause different types of damages that might lead to significant financial losses [18]. Information security damages can range from small losses to entire information system destruction.

The process of developing an effective information security policy is straight forward which is shaped by threats to an information system, the information systems security policy defines the objectives of the information system of an organization and outlines a strategy to achieve these stated objectives [44].

According to many scholars information security threats are broadly classified in to three categories as **natural threats**, **physical security threats** and **human threats**. Natural threats include natural disasters such as earthquakes, hurricanes, floods, or any nature-created disasters that cannot be stopped. Information damage or lost due to natural threats cannot be prevented as no one knows in advance that these type of threats will occur. However we can implement a few safeguards strategies against natural disasters by adopting disaster recovery plans and contingency plans. Physical threats may include loss or damage of system resources through fire, water, theft and physical impact. Physical impact on resources can be due to a collision or other damage, either intentionally or unintentionally. Human threats include threats of attacks performed by both insiders and outsiders. Insider attacks refer to attacks performed by disgruntled or malicious employees. Outsider attacks refer to attacks performed by malicious people not within the organization. Insider attackers can be the biggest threat to information system as they may know the security posture of the information system, while outsider attackers apply many tricks such as social engineering to learn the security posture of the information system.

Here is some list of the most common threats that can jeopardize the confidentiality, integrity, and availability of any organization's information assets.

Hackers

Hackers are among the most well known outside threats to information systems. Most people may say about hackers as they are geniuses, but in reality, they are nothing more than persistent individuals who have sufficient time to learn their craft [42]. Hackers can be divided into three types according to many researchers these are Hackers, Crackers, and Phreakers.

Hacker can be defined as an individual that breaks into computer systems to learn more about them. They generally do not intend harm or expect financial gain; however, they may un intentionally pass on valuable information to others, which could damage systems. In other words hackers are that individual who seek and exploits information systems or network vulnerabilities.

The term Cracker refers to the "criminal hacker" they are just like hackers but there intent differs. These individuals intend to do harm to information systems, while their motives may vary.

The term Phreaker refers to an individual who prides himself or herself on compromising telephone systems, network systems and information systems. They have been known to reroute phone lines, disconnect phone lines, sell wiretaps, etc.

Viruses/Trojans/Worms [18]

A computer Virus is embedded code or attached to a file where it infects the computer when the file is executed. Viruses are spread through users transferring files, usually unknowingly, through e-mail or file sharing. Even if we download the infected file the Virus cannot act until the malicious file is executed, which means it won't harm our computer until we run it. The only way a Virus can spread is through user involvement; it cannot execute or transfer itself independently. It can infect other files on our machine however, it cannot replicate itself.

A computer Worm is similar to a Virus by design and is considered a sub-class of a Virus. The difference is that a Worm gains access to our systems transport features and is able to travel unaided by the user. A Worm also has the added ability to replicate itself, so instead of sending out a single Worm it can send out hundreds and thousands of copies of itself creating a continuous cycle. Because of its ability to reproduce it can end up using tons of system memory and bandwidth causing servers and individual systems to crash. Unlike a Virus, it cannot infect other files on our computer.

Typically a Trojan will appear to be a useful and legitimate application from a legitimate source and could possibly promise to clean our system of viruses or search our registry for spyware. When we execute a Trojan the results could vary from as little as changing our desktop wallpaper, creating annoying pop-ups, or to the extreme of deleting and destroying files and programs. Trojans are also known for creating backdoors to our system that allows malicious users to gain access to files and information. Unlike a Virus or Worm, a Trojan cannot infect other files or replicate.

In short computer viruses are modifications made to existing program files that duplicate on their own. Trojans are programs that infect systems by taking advantage of unsuspicious end users that believe they are playing a familiar game or reading email attachments. Worms differentiate themselves by having the ability to replicate. They typically take advantage of LAN and email clients. According to different scholars the best defense is still properly implemented anti-virus software and a sound policy to enforce it. While there are countless vendors that offer anti-virus software, we should take our time to thoroughly research which software will complement the organization's needs [42].

Denial of Service (DoS)

DoS is an attempt to make a computer or network resource unavailable to its intended users. This could be CPU resources, but often involves efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. It is an attack

which usually attempts to deny a user, or group of users, the ability to use a particular service.

Denial of service attempts may be intentional by flooding a network to prevent traffic or unintentionally by using a company server to store large amounts of software, thus denying access to that server [42]. A variation of this tactic is called the distributed denial of service (DDoS). This particular method uses several servers to attack other machines. It can be difficult to identify this type of attack because the traffic may look like valid access attempts.

Both DoS and DDoS attacks can disrupt network connectivity, hog bandwidth, turn company resources against it, etc. A few options to consider when planning for this situation is writing a policy by properly configured router filters, TCP SYN flooding patches, disabling network services that are not used, and observing machine performance create baselines for normal activity [42].

Social Engineering [42]

Social engineering is a technique which is used to breach security that does not require a computer or any software. There are many definitions to describe social engineering, most agreeing on one thing: gathering information that grants access to systems for malicious intent.

Social engineering is similar to hacking, but it manipulates individual's trust to gain their information rather than manipulating company resources. It may be accomplished through several methods like telephone, social network sites, dumpster diving etc. We have to make sure to add a policy for destroying (shredding is good) any and all sensitive information in case of dumpster diving. There are many other types of social engineering, such as on-line social engineering and simple persuasion that need to be guarded against. This is an issue that is typically overlooked. We have to make sure to outline, in detail, preventative measures against social engineering attacks.

Insider threats

Insider threats are employees of network participants that have malicious intentions of disrupting the network or stealing information for their personal benefit. Personal motivational reasons often include low wages and working environment, affiliation with a competitor or terrorist organization, or personal benefits, for example due to predictive stock market reactions [47].

Users are among a very common but overlooked security threat. It has been argued that protecting from the inside is more important than the outside. While most incidents regarding end users are unintentional, they can still cause a disastrous situation. Chat rooms, games, real player, real audio, etc all open up certain ports for communication which can lead to an entry point for an intruder [42]. End users also tend to write down user names and passwords and hide them under their keyboards, in their desks, or some other place easily accessible to other individuals. A good example here is a disgruntled employee who might go around after hours looking for this type of information. He/she might use it themselves or pass it on to a potential hacker. Addressing these issues in an end user training policy and/or an acceptable use policy can be implemented here to mitigate these risks. It is advisable to have employees sign off on acceptable use guidelines to make certain they are aware [30].

Insiders are particularly dangerous, as they can have the full knowledge of the internal system of an organization and the resources at their disposal to run an extensive and well prepared attack. They have a trusted status within one organization and can exploit this to harm either the whole system (including the organization they work for) or specific targets. Unlike other attacker types, insiders do not need to rely on finding vulnerabilities. Instead, they can abuse their privileges or attack the network via hidden attacks. Attack situations may become particularly attractive if observation and therefore punishment is difficult or unlikely [16]. Entry points for attacks usually come from within an organization and can consist of both remote and local proximity attacks.

Although technical aspect of information security needs due attention, a more serious and underrated aspect of information security is the human element [30]. The evolving trend in information security triggers the incorporation of the human element in ensuring information security of an organization. Promoting a sustainable information security culture is an effective way for organizations to address this aspect of information security. As the banking sector in Ethiopia is undergoing fast progress in migrating business processes towards new IT-based services, the idea towards establishing and maintaining sustainable information security culture become more appropriate now than ever [27].

Firewalls and intrusion detection systems are powerless and largely irrelevant when it comes to protecting information assets within the organization. Instead, new security mechanisms must be integrated into enterprise applications and the rest of the infrastructure. These mechanisms include stronger authentication, access control, audit trails, host-based intrusion detection and encryption technologies, all of which serve to make information available to those who have a legitimate need to access it, while keeping others safely away [36].

People (or employees) in organizations know that security cannot be achieved by just installing technical solutions like IDS, firewalls and implementing processes. Because it is the people in turn in these organizations, who maintain the technology, maintain the day-to-day security processes and influence the security culture of their organizations. So it is important to focus on people factor to measure the security culture, security awareness and how information security is managed in these organizations [37].

2.1.1.5. Information Security Awareness

Information Security Policies are necessary to ensure that important data, business plans and other confidential information are protected from theft or unauthorized disclosure. If employees of any organization are not aware of these policies, they will not know what is expected of them when they handle such confidential information [48].

Every organization should have well taken care of organizations information assets but if the staffs are not educated on Information Security Policies, their lack of education, awareness and training would result in confidential information simply walking out the front door [48].Therefore, it is very important that Information Security Policies be implemented and that all staff is educated and trained in these policies.

In today's business environment most of the companies rely on electronically exchanged information. It is a requirement of all the departments to produce and pass information across different departments in a quick and secure manner to support their business activities. Information plays an important role in making decisions. Therefore commercial companies have different classification of data based on its importance and use [18].

Business success depends upon continuity of operations and information provided to the business processes by information systems. The growth, excellence and efficiency of the business could be damaged due to the threats and misuse of information. Therefore, awareness program basically helps, set measures and educate users on how to behave and get benefit out of information without jeopardizing its confidentiality, integrity and availability. Employees are the primary users of the information [19]. A lack of awareness and mishandling of information could expose this information to competitors or get corrupted. If this information is freely available the following could be some of the impacts on the company and its business functions:

- The information available easily can be used by competitors to design strategies and launch new products with more features
- The company's credibility can be affected from this disclosure
- Customer confidence can be lost
- Help competitors to gain more share in the market
- Suppliers and partner would be conscious to deal with the company
- Noncompliance's to government and industry laws and standards
- Employees will lose trust and will look for other opportunities

2.1.1.6. Information Security Governance

Different scholars try to define information security governance but it has not been reached on a consensus [14]. As [34] "information security governance is the establishment and maintenance of the control environment to manage the risks relating to the CIA of information and it's supporting processes and systems". As [35] Information security governance is all of the tools, personnel and business processes that ensure that security is carried out to meet an organizations specific needs, it requires organizational structure, roles and responsibilities, performance measurement, defined tasks and oversight mechanisms.

The foundation of a successful information security program begins with strong upper-level management support. Without a solid support of the persons at higher positions that controls IT resources, the effectiveness of a security program can fail when pressured by some company politics and budget limitations [29]. As [29]"Any information security program must get its direction from executive management". The other component of an effective security program is practical security policies and procedures backed by the authority necessary to enforce compliance. Practical security policies and procedures are defined as those that are attainable and provide meaningful security through appropriate controls [29]. The ability to capture and provide meaningful information is the other component of effective security program. The success of an information security program implemented should be judged by the degree to which meaningful results are produced. The program must meet the needs of the organization and not just be an implementation of commonly developed controls. All security decisions must be linked to the organization's business objectives and mission statement [29].

A security governance to be successful, security policies and procedures in the program must have three key elements; they must be documented, communicated and current. To supplement an information security policy, the organization must offer awareness programs, user training and support education [30].

The typical driver of information security governance in the banking sector is the prevention of financial fraud through the manipulation of an organization's electronic

data[34]. Attempts to prevent abuse and fraud have led to increased regulations, standards, and guidelines, causing organizations to pay greater attention to governance, which has changed the dynamics of information security management [19]. Computer crimes and cyber-attacks are on the rise, many of which are perpetrated by the use of social engineering techniques. Building security awareness into the governance structure has become essential. Information security professionals are faced with ever-evolving technologies, sophisticated and determined cyber criminals, a blended threat landscape, and increased compliance requirements based on new corporate governance initiatives.

Information Security Governance Frameworks

- ✓ **ISO 27000 Series [9]:** The International Organization for Standardizations (ISO), established in 1947, it is a non-governmental international body which collaborates with the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU)on ICT standards. The ISO 27000 series of information security standards provides a set of frameworks for developing a security program from concept to maturity. It's broken up into several parts in order to be manageable, 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 ISO/IEC 27000 series is a comprehensive set of controls comprising best practices in information security. It is an internationally recognized information security standard, broad in scope and generic in applicability. It focuses on risk identification, assessment and management. It is aligned with common business goals:

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

ISO/IEC 2700 series is about information security, not IT security. It is much more commonly applied in commercial organizations than in government.

- ✓ **COBIT[32]:**COBIT is a set of IT management practices published by ISACA(Information Systems Audit and Control Association).ISACA is a widely recognized independent IT governance organization, and its COBIT guidelines are used by IT management in many organizations to define and manage processes based on a maturity model like the Capability Maturity Model (CMM). COBIT is not about information security, it is a general IT standard, but certain security practices are embedded within it. COBIT contains a higher-level set of information security guidelines than the ISO 27000 series, intended to align business goals with IT goals.

  ISACA periodically updates the COBIT processes and releases new versions. COBIT 5 is the current version, which is organized from five conceptual areas Plan, Do, Check, Adjust, and Governance. It includes best practices, processes and measures organization can implement to standardize IT management. It is generally considered as complimentary to ISO/IEC 2001 and 27002.

- ✓ **NIST 800 series [33]:** The National Institute of Standards and Technology (NIST) provides a set of "Special Publications" to assist industry, government, and academic organizations with following best practices. Known as the "800 series," the set of security-specific publications is very specific to individual technologies, with the exception of 800-53.800-53 was developed primarily for the U.S. Federal Government, to specify security control organization and structure, security control baselines, common controls, security controls in external environments, security control assurance, risk management, information system categorization, security control selection, and monitoring of security controls.800-53 is organized into 18 "security control families," which are conceptual categories that represent important components of a complete security program.

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

- ✓ **PCI DSS [31]:**PCIDSS is one of the world wide information security standard which is 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. It helps the organizations to process card payments and to prevent 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, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process.

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 antivirus software or programs 6. Develop and maintain secure systems and applications
Implementing Strong Access	7. Restrict access to cardholder data by business

Control Measures	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 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

Table 1: PCI DSS High Level Overview (From PCI DSS)

PCI DSS is applicable in current Ethiopian PSS member banks which are 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.

All information security governance frameworks have an Information Security Policies, Procedure and Standards as one of the most basic requirements.

2.1.2. Overview of Information Security Policy

The four components of security documentations are policies, procedures, standards and guidelines [5].

- Policy is a high-level statement of requirements. It is the primary way in which management's expectations for security are provided to the builders, installers, maintainers and users of an organizational information systems.
- Standards specify how to configure devices, how to install and configure software, and how to use computer systems and other organizational assets, to be compliant with the intentions of the policy.
- Procedures specify the step-by-step instructions to perform various tasks in accordance with policies and standard.

- Guidelines are advice about how to achieve the goals of the security policy, but they are suggestions, not rules. They are an important communication tool to let people know how to follow the policy guidance, it conveys best practices for using technology systems or behaving according to management's preferences.

A security policy is a document or set of documents that describes the security controls that should be implemented in the company at a high level for safeguarding the organization's information from inside and outside attacks [5]. It defines the complete security architecture of an organization and the document includes clear objectives, goals, rules and regulations, formal procedures, and so on. It clearly mentions the assets to be protected and the person who can log in and access data, who can view the selected data, as well as the person who are allowed to change the data, etc. Without these policies, it is impossible to protect the company from any possible threats.

Security Policies are the foundation of the security infrastructure [5]. These policies secure and safeguard the information resource of an organization and provide legal protection to the organization. These policies are beneficial since they help bring awareness of the staff working in the organization to work together to secure its communication, as well as minimizing the risks of security awareness through human-factor mistakes such as disclosing sensitive information to unauthorized or unknown sources, improver use of internet, etc. In addition, these policies provide protection against cyber-attacks, malicious threats, foreign intelligence, and so on. They mainly address physical security, network security, access authorization, virus protection and disaster recovery.

All policies need to be supported by relevant security standards, procedures and guideline documents[18].

2.1.2.1. Purpose of Information Security Policy

The broad aim of the information security policyis to provide a better secure environment. A good security policy should outline responsibilities of individuals, define penalties for violations and provide a mechanism for updating the policy [12].

The ISP has an important role to play in emphasizing management's commitment and support for information security. While the ISP provides the framework for facilitating 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 [44].

In recent years, a consensus has emerged both within the academic and practitioner communities that the security of corporate information resources is predicated upon the formulation and application of an appropriate information security policy (e.g., Rees et al., 2003). As [12] stated, the information security policy is now a mandatory for an effective security management. Without ISP the organization may face lots of problems regarding information security. In a similar ways [5] stated that the ISP is the heart and basis of successful security management. However, while the ISP may play an important role in effective information security management, there is growing recognition that the policy is unlikely to be a successful security tool, unless organizations adhere to a number of important prescriptions in their policy implementation [18], as an example the policy must widely and strongly disseminated throughout the organization, the policy must be reviewed and revised frequently.

Security policies serve as informing employees of the guidelines that protect company information and assets. A well-written policy will provide acceptable use and prohibited use guidelines, which will automatically reduce risks if employees abide to the policy. Security policies also serve as a good foundation for conducting audits of the network and its resources. It serves as a baseline to follow when trying to uncover vulnerabilities or when conducting forensics activities if security has been breached.

Developing a security policy will help define strategic goals, identify critical assets, and uncover potential vulnerabilities or existing vulnerabilities [29].

[39]Information resources can retain their integrity, confidentiality, and availability only if they can be protected from the growing range of threats that is arrayed against them.

The objectives of policy are [5,18, 42]

- Ensure the protection of information systems and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- Provide a safe and secure information systems working environment for employees and any other authorized users.
- Make certain that all authorized users understand and comply with the policy and any other associated policies, and also adhere to and work within the relevant codes of practice.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Protect the organization from liability or damage through the misuse of its information systems facilities.
- Ensure business continuity of the organization
- Comply with the law and defend ourselves against legal action
- Maintains an organizations reputation
- To protect the organization's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability.
- To establish safeguards to protect the organization's information resources from theft, abuse, misuse and any form of damage.
- To establish responsibility and accountability for Information Security in the organization.

- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of Information Security incidents.
- To ensure that the organization is able to continue its commercial activities in the event of significant information security incidents.
- To strengthen internal control and prevent unauthorized and improper access to data, thereby ensuring the appropriate protection of information assets
- To appropriately protect the confidentiality and integrity of information assets
- To ensure that information is not revealed to unauthorized third parties during the process of transmission or as a result of unintentional actions
- To ensure that all information security accidents or suspected security flaws have appropriate reporting mechanisms so that any incidents are appropriately investigated and handled

2.1.2.2. Fundamentals of Information Security Policy

Security policies are beneficial since it is the foundation of a security program as many scholars stated. Without policies, an organization's security program will be short lived [42].

A sound security policy starts with the executives commitment and support at the top. Without management supporting security policies, it is better to consider it as non-existent. In most instances, management is ultimately responsible for setting the "tone" for a sound security infrastructure [42].

The cornerstone of effective information security architecture is a well written policy statement. This is the source from which all other documents like standards, procedures, guidelines, and other supporting documents will be produced [42].

As with any foundation, it is important to establish a strong footing. A policy performs two roles, one internal and one external. The internal part tells employees what is expected of them and how their actions will be judged. The external part tells the world

how the enterprise is run. Every organization must have policies in place that support sound business practices and they will demonstrate to the world that this organization understands that protection of assets is vital to the successful execution of its mission [34].

In any discussion regarding written requirements, the term "policy" has more than one meaning. To some, a policy is senior management's directives on how a certain program is to be run, what its goals and objectives are, and to whom responsibilities are to be assigned. Policy may refer to the specific security rules for a particular system. Additionally, policy may refer to entirely different matters, such as specific management decisions setting an organization's e-mail privacy policy or internet usage Policy [44].

Security and privacy policies and procedures must have three elements to be effective. They must be documented, communicated, and current. The actual physical format (layout) of the policy will depend on what policies look like in our own organization. To be successful, it is very important that any policy developed look like published policies from the Organization. Some members of the review panel will be unable to read and critique the new policy if it does not look like a policy. Policies are generally brief in comparison to procedures.

There are three types of policies, and we will use each type at different times in our information security program and throughout the organization to support the business process or mission. The three types of policies are [18]:

1. Global or Program (tier 1): these are used to create the organization's overall vision and direction.

2. Topic-Specific or Issue-Specific(tier 2): these address particular subjects of concern.

3. Application-specific policies: these focus on decisions taken by management to control particular applications.

The roles and responsibilities of the all information systems users are also addressed in the policy document in order to ensure the protection of confidentiality, availability and integrity of information assets of the organization. The policy must

mention management's objectives and expectations for information security clearly, in detail along with the implications of noncompliance.

The existence of the policy documents heavily depend on the management's dedication and adherence to information security [39]. Application and relevance of the policy document need to be reviewed and updated in pre-set time lapses. In most of the organizations reviewing is done once a year, while other organizations concerned about information security do it in more frequently. Failure to keep the policy up to date reflects lack of management's commitment or the failures in processes to organizational governance.

According to [9, 33, 42], the following principles should be considered in to account for formulating and developing and effective security policy.

- Develop policies that we plan to enforce: A policy that we are unable or unwilling to enforce is useless.
- Explain the purpose of the policy: policies should be developed with specific objectives in mind. We have to be sure the need for the policy and specify what the policy is trying to accomplish.
- Develop security policies that do not require updates too frequently: if our policies require frequent update we are probably kept ourselves in developing policies only, we cannot do other important tasks.
- Differentiate between policies and standards or recommendations: our policies should be comprehensive and should not be so specific or detailed.
- Since our security policies will apply to all employees across the organization, it is a good idea to include employees from other departments in their development
- Make our security policies available to everyone: a policy that is not available to employees would not be effective.
- Make sure our security policies stays current: policies cannot last forever without some modifications. Current situations might be different from the one that time, where policies weredeveloped.

- Make sure our policies are understood: we have to develop policies that can be easily understood. If employees cannot understand what the policy requires, they might not comply with the policy. For example a policy that is too long or complex will most likely never been read and certainly will not be followed.
- Require acknowledgement of our policies: employees has to sign when receiving a copy of the policy, that they have read the policies and that they agree to abide by the policies.
- Determine upfront what is required to make a policy "official": policies that apply to the entire organization typically require approval from multiple levels within the organization.
- Make sure our legal department is involved: since our security policies are extremely important in protecting our organization and since failure to follow the policies could cause severe damage to the corporation and loss of employment to the employee, we have to make sure that we obtain our legal department's review and approval of all policies.

2.1.2.3. Common Information Security Policies [9, 42, 30]

Access Management Policy: the purpose of this policy is to state access controls, which limit the actions or operations that legitimate user of a data and computer system can perform. It constraints what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In other words it helps for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an access control program.

The policy serves as the blueprint for the management of user access authorizations and control mechanisms for computer networks, operating systems, applications and information.

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by the enterprise; it can be specific application, physical access of data center, entrance to the enterprise.

Acceptable Usage Policy: the purpose of this policy is to define acceptable and unacceptable usage of information assets and information processing facilities within the organization. These rules are in place to protect the employee and the company from in appropriate use exposes to risks including virus attacks, compromise of network systems and services, and legal issues. The enterprise may provide computers, network, and some other electronic information systems to meet its goals and missions, so this policy could states that there must be a proper use of those devices and information systems to maintain the confidentiality, integrity and availability of its information assets.

The scope of this policy is applicable to all employees, contractors, consultants, temporary and other workers at the enterprise, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by the enterprise.

Network Security Policy: the purpose of this policy is to ensure the availability of an effective, highly available network or in other words to establish a clear and straight forward direction to protect business information transmitted to and from the organizational environment through the organizations network and to protect information systems and facilities that can be used in the organizational network.

This policy will assist in ensuring the availability of an effective, highly available network. It provides formal responsibilities for taking measures against devices that threaten the stability, integrity and security of LSE's network. It will facilitate the rapid tracking down and resolution of problems

related to LSE network connected devices by Information Management and Technology

The scope of this policy will include all information and information systems that transmit, share, process or store information through organizational networks.

Data/Information Handling Policy: the purpose of this policy is to achieve and maintain appropriate protection of the organization's information and information system assets. The other purpose is to establish a framework for classifying and handling the enterprises data based on its level of sensitivity, value and criticality to the enterprise as required by its information Security Plan and to establish a comprehensive data security program in compliance with applicable law. Classification of data will aid in determining baseline security controls for the protection of data.

In general it is designed to establish processes for ensuring the security of confidential information and to establish administrative, technical and physical safeguards to protect against unauthorized access or use of this information.

This policy could outline essential roles and responsibilities within the enterprise employees for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests.

The scope of this policy could be to all enterprise employees or third parties who access, process, or store sensitive data.

Internet Usage Policy: the purpose of this policy is to state the usage of internet within the organization. Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital

information assets. These risks include: Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may affect the productivity of individuals due to time spent using or surfing the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

The scope of this policy is applicable to all Internet users within the enterprise who has access the Internet through the computing or networking resources, it could be permanent employees, contract workers, temporary agency workers, business partners, and vendors. The company's internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services internet access is to be used for business purposes only.

E-mail Security Policy: the purpose this policy is to ensure the proper use of email system and make users aware of what the enterprise's acceptable and unacceptable use of its mail system. It intends to set appropriate control that can prevent the organization from any damage that may possibly occur through email communication.

Electronic mail is pervasively used in almost all industry and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

The scope of this policy may be applicable to all employees, vendors, and agents operating on behalf of the enterprise.

Personnel Security Policy: the purpose of this policy is to help the enterprise in implementing best security practices with regard to personnel screening,

termination, transfer and management. This Security policy serves to be consistent with best practices associated with organizational Information Security management.

Management and personnel have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish management responsibilities, education, training and formal processes to handle problematic security situations.

The Personnel Policy sets out the processes and responsibilities that are necessary to ensure that the staff of an organization contribute to the security of its information [40].Depending on their role within the organization, different individuals will have different levels of responsibility for information security, but in all cases these responsibilities need to be defined and individuals given appropriate training and support to enable them to fulfill their responsibilities.

Password Usage policy: passwords are methods that facilitates authentication, it is important to avoid unauthorized user access for information systems. The purpose of this policy is to enforce employees to set a minimum requirement for password usage; this can be forcing users to change their password frequently, to prompt complex password which cannot be guessed or cannot be accessed by brute-force attacks easily, not allowing users sharing passwords etc…

The scope of this policy is applicable to all employees within the organization who has a computer or any information system access.

Encryption Security Policy: the purpose of this policy is to ensure all business critical information that is stored and transmitted on the organization's information systems shall be encrypted using strong cryptographic algorithms.

Unauthorized access to sensitive information can have significant detrimental effects on individuals or the institution. There have been different kinds of information security breaches at every enterprises which resulted from the loss or theft of laptops or other portable devices and media. Desktop computers and devices also pose a significant risk due to the difficulty of providing adequate and consistent physical and network security. Hence we can protect such kind of losses due to some encryption mechanisms so it reduces the risk of unauthorized access to any remaining sensitive information. Therefore encryption policy defines the acceptable use and management of encryption software and hardware throughout the enterprise.

The scope of this policy is applicable to all the enterprise users who works on critical information or data as well as any critical information systems.

Malicious Software Protection Policy: the purpose of this policy is to protect from malicious software like virus, worm, Trojan horses etc. which can cause loss of data, degrading efficiency of computing devices and opening backdoors for security threats that may expose the organizations for a number of computer security incidents and the resulting cost of business disruptions. In other words this policy intends to set solid controls to prevent vulnerability for virus attacks.

This policy establishes requirements necessary for maintaining the confidentiality, integrity and continuous availability of data and network resources at the enterprise. Software sometimes known as malware is designed to penetrate and/or damage systems without the owner's awareness and

consent. Examples include: computer viruses, worms, Trojans, spyware, and rootkits.

The scope of this policy is applicable to all employees whose work is on computing devices.

Backup and Restoration Policy: the purpose of this policy is to establish the rules and procedures for good working practices for the backup and restoration of electronic information as well as any enterprises information assets.

Enterprises must ensure that all information and data which it is responsible for is securely and routinely backed up. The enterprise has to ensure that information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances.

The scope of this policy extends to the back-up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure.

Hardware and Software Acquisition, Development and Maintenance Policy: the purpose of this policy is to state how hardware and software acquisition will be performed by employees of the enterprise according to information security requirements in the organizations business environment.

Any employee who wants to purchase a software or hardware in support of their mission, the purchases are coordinated with the IT department, so that the technology will be secured, compatible with the infrastructures and the enterprises systems. The aim of this policy is to inform employees in the purchase and acquisition of software and hardware based on some hardware and software acquisition and purchasing procedures and guidelines.

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment [42].

It seeks to prevent situations where departments or administrative units purchase systems or software (that require IT resources and support to operate) without informing IT and then expect IT to support such systems. IT resources and support refers to programming, systems administration, networking, consulting, training, Helpdesk troubleshooting and break/fix support

Data Center Security Policy: the purpose of this policy is to promote access and physical security controls that safeguard equipment, personnel, and data in data center and mission critical facilities. This policy states that only those persons can enter into the data center, who has the privilege.

The procedures described in the document could have been developed to maintain a secure Data Center environment and must be followed by people working in the Data Center. It is important that any department/project contemplating the installation of their Servers in the Data Center fully understand and agree to this policy.

Physical and Environmental Security Policy: the purpose of this policy is to identify the measures adopted by the organization for protecting the information assets from physical and environmental threats. Physical and environmental security refers to controls taken to protect information systems, the office building and related supporting infrastructure against threats associated with their physical environment.

Incident Management Policy: the purpose of this policy is to identify and resolve information security incidents quickly and effectively, minimize their business impact and reduce the risk of similar incidents occurring in the future.

Everyone has an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security

This policy aims to support the prompt and consistent management of information security incidents in order to minimize any harm to individuals or the organization. To this end all users and managers of organizations information and IT systems need to understand their roles in reporting and managing suspected incidents report actual or suspected information security incidents promptly, following the procedures

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts continually improve and strengthen the information security infrastructure of the Province.

Change Management Policy: the purpose of this policy is to manage changes in a rational and predictable manner so that users and third parties can plan accordingly. Change requires serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resources.

Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalized governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This

formalization requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on IS's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organizations can demonstrate increased agility in responding predictably and reliably to new business demands.

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk.

2.2. Related works

[49] Studied information security challenges in relation to enterprise security polices in the financial sector of Srilanka. The research was carried out on private commercial banks in the country. The purpose of the research was to gain a better understanding of the information security challenges faced by the financial sector in Srilanka. Most of the banks in the country does not consider information as a valuable asset. Some of the banks does not have a proper information security policy, which is one of the vulnerabilities.

[4] Assesses Information Security Management in Ethiopian banks, and the researcher found that there is lack of formalized comprehensive ISM framework. So the researcher proposed ISM framework for Ethiopian banks, the proposed framework has two major components security requirement identification method and the counter measures for threats. The research examines and compares information security elements from the commonly used information security governance frameworks, and best practices.

[50] Assesses internet bank security in Ethiopian banking industry and they proposed a security framework. The framework enables banks to have a standardized approach of addressing internet banking security by realizing the holistic approach of security requirements. The proposed framework has two layers, outer and inner layer, the outer layer comprises of national regulatory bodies which are NBE, INSA, FIC and ECER^{2}T. The inner layer consists of five major models which are, internet banking customer site security model, internet banking AAA model, internet banking risk management model, internet banking security defensive and offensive model and security checklist.

According to [15] information security is not only a problem that technology can address alone, but also a problem a management to solve. Therefore legal frameworks in the form of policy and standards are the most prerequisites to establish efficient and reliable security governance systems.

[27] Assesses the practices of information security culture in Ethiopian banking industry; they found that the level of information security awareness in the sector is unsatisfactory. The aim of the research is assessing the practices of information security culture, by identifying key problems in order to figure out the gap that needs managements and policy intervention for establishing a good information security culture. The major findings of this research are the need for effective information security awareness, trust environment and communication to promote sustainable change in information security culture which enables proper information security governance and implementation that complies with local and international standards.

[28] Assesses factors that affect the adoption of E-banking in the Ethiopian banking industry. The researcher employs mixed research approach, and it is conducted in four banks. The study revealed that the major barriers in the adoption of electronic banking in Ethiopian banking industry are; security risk, lack of trust, lack of legal and regulatory framework, lack of ICT infrastructure and absence to competition between local and foreign banks. The study suggests a series of measures which could be taken by the banking industry.

[51] Examines insider threat management of Ethiopian banking industry with particular emphasis on the insider threat, assessing the factors that leads insider to commit malicious activities and mitigation strategies for malicious insider threats. The research is based on surveys of all Ethiopian banks. The research revealed that insider threats like the installation of unauthorized software threat and financial frauds are the most frequently happening threats. According to the study dissatisfaction with immediate reporting manager, steal data for monetary gain, desire for recognition, and emotional distress are among motivations for insider threats. The study provides recommendations and best practices from different literature review to mitigate those insiders malicious activities within the Ethiopian banking industry.

Chapter 3 Research Methodology

In order to achieve the objective of this research the following research methods are used. This chapter addresses the research design, the study population, data collection methods, methods of data analysis and outline of the interview.

3.1. Research Design

Researchers can use different types of design depending on the type of problem, the knowledge already available about the problem and the resources available for the study. For the purpose of this research qualitative kind of research methodology is selected. Structured in-depth interview is used as a collection method. The research looks in to the practices of Information Security and ISP, and the challenges regarding ISP in the Ethiopian banking Industry.

Qualitative data collection and analysis usually proceed simultaneously; ongoing findings affect what types of data are collected and how they are collected. Making notes as the data collection and analysis proceed is one important data analysis strategy. The notes, or possibly sketches, trace the thinking of the researcher and help guide a final conceptualization that answers research questions (or related ones) and offers a theory as an explanation for the answers. There is less consensus among qualitative researchers about designs as that of quantitative researchers [39].

The research is descriptive type of research, which tries to present the current information security and information security policy practices with regard to Ethiopian banking industry.

3.2. Study Population

There are sixteen private, three government owned banks and one central bank in Ethiopia. For the purpose of this research, one central bank which is National Bank of

Ethiopia, three governmental banks which are Commercial Bank of Ethiopia, Development Bank of Ethiopia, Construction and Business Bank; seven banks from the private banking sector which are: Awash International Bank, Dashen Bank and Bank of Abyssinia, Wegagen Bank, United Bank, Oromia International Bank and Zemen bank are selected based on their ages since their establishment sand their market share in the country. Nib banks were one of the banks that should be included in the list but they are not willing to collaborate for the research. Zemen bank is chosen because of its uniqueness in service giving, it is the only one branch bank based service.

The sample consists of more than half of the total population. The criteria for selection of the banks is based on the year of establishment (the researcher assumes that the more the number of years, the more stable the bank and the more they have experience on the subject matter) and based on their capital share in the country as we can see in Table 1 below from 2013/14 National Bank of Ethiopia's report.

Banks	Branch Network								Capital			
	2012/13				2013/14				2012/13		2013/14	
	Regions	Addis Ababa	Total	% Share	Regions	Addis Ababa	Total	% Share	Total Capital	% Share	Total Capital	% Share
1. Public Banks												
Commercial Bank of Ethiopia	595	137	732	42.4	700	156	856	38.8	9,027.0	38.7	9,045.0	34.2
Construction & Business Bank	63	42	105	6.1	68	47	115	5.2	465.0	2.0	642.1	2.4
Development Bank of Ethiopia	31	1	32	1.9	31	1	32	1.4	2,554.0	10.9	2,134.8	8.1
Total Public Banks	**689**	**180**	**869**	**50.3**	**799**	**204**	**1003**	**45.4**	**12,046.0**	**51.6**	**11,821.9**	**44.7**
2. Private Banks												
Awash International Bank	47	67	114	6.6	62	90	152	6.9	1,628.0	7.0	1,979.3	7.5
Dashen Bank	59	53	112	6.5	69	73	142	6.4	1,493.0	6.4	1,994.1	7.5
Abyssinia Bank	41	45	86	5.0	55	54	109	4.9	909.0	3.9	1,326.0	5.0
Wegagen Bank	38	41	79	4.6	51	49	100	4.5	1,570.0	6.7	1,825.8	6.9
United Bank	30	45	75	4.3	44	55	99	4.5	951.0	4.1	1,334.4	5.0
Nib International Bank	30	42	72	4.2	39	55	94	4.3	1,453.0	6.2	1,731.3	6.5
Cooperative Bank of Oromiya	62	12	74	4.3	84	21	105	4.8	549.0	2.4	739.9	2.8
Lion International Bank	23	22	45	2.6	35	27	62	2.8	415.0	1.8	514.3	1.9
Oromia International Bank	44	21	65	3.8	80	29	109	4.9	490.0	2.1	594.3	2.2
Zemen Bank	3	5	8	0.5	3	6	9	0.4	400.0	1.7	529.1	2.0
Buna International Bank	20	13	33	1.9	41	22	63	2.9	321.0	1.4	446.6	1.7
Berhan International Bank	11	11	22	1.3	22	26	48	2.2	340.0	1.5	488.7	1.8
Abay Bank	37	10	47	2.7	54	16	70	3.2	300.0	1.3	395.0	1.5
Addis International Bank	2	9	11	0.6	5	16	21	1.0	205.0	0.9	277.9	1.1
Debub Global Bank	10	4	14	0.8	12	7	19	0.9	114.0	0.5	177.3	0.7
Enat Bank	0	2	2	0.1	0	3	3	0.1	162.0	0.7	261.6	1.0
Total Private Banks	**457.0**	**402.0**	**859.0**	**49.7**	**656.0**	**549.0**	**1,205.0**	**54.6**	**11,300.0**	**48.4**	**14,615.4**	**55.3**
3.Grand Total Banks	**867**	**582**	**1728**	**100**	**1455**	**753**	**2208**	**100.0**	**23,346.0**	**100.0**	**26,437.3**	**100.0**

Table 2: Directly taken from National Bank of Ethiopia's (2013/14) Report on Ethiopian Commercial Banks

3.2.1. Overview of selected banks

National Bank of Ethiopia (NBE): The National Bank of Ethiopia was established in 1963 by proclamation 206 of 1963 and began operation in January 1964. Prior to this proclamation, the Bank used to carry out dual activities, i.e. commercial banking and central banking. The proclamation raised the Bank's capital to Ethiopian dollars 10.0 million and granted broad administrative autonomy and juridical personality. Following the proclamation the National Bank of Ethiopia was entrusted Ethiopian banks regulatory body.

Commercial Bank of Ethiopia (CBE): is established in 1942 and it is the current leading commercial bank in Ethiopia, CBE is also a pioneer in the introduction of most modern banking technologies.

Construction and Business Bank (CBB): is established in 1975 through the merger of two financial institutions which are Imperial Savings and Home Ownership Associations, and Savings and Mortgage Corporation of Ethiopia. CBB is a wholly government-owned public enterprise bank.

Development Bank of Ethiopia(DBE): is established in 1909, it has played a significant role in promoting overall economic development of the country. DBE is one of the financial institutions engaged in providing short, medium and long term development credits.

Awash International Bank (AIB): is established in 1991 and it was established by 486 founder shareholders with a paid up capital of 24.2 Million. Its headquarter is located in Addis Ababa. It has 181 branches currently.

Dashen Bank: is established in 1996, it was established under the proclamation of Ethiopian commercial code of 1960's. Its' headquarter is located in Addis Ababa. It operates through a network of 146 area banks, nine dedicated Forex Bureaus, 170 ATMs and more than 834 POS (point of sales).

Bank of Abysisinia: is established 1996. it started its operation with a paid up capital of 67.8 Million Birr with 131 shareholders and 32 staff.

Wegagen Bank: is a privately owned company which starts its operations in 1997 with a subscribed capital of birr 60 Million and capital of birr 30 Million. Its head quarter is located in Addis Ababa. The number of shareholders reached 2,262 and the total capital reached over Birr 2.3 Billion as March 31, 2015.

United Bank: is established in 1998 in accordance with the commercial code of Ethiopia 1960.United Bank is a full service Bank that offers its customers a wide range of commercial banking services with a network of 125 branches, and a number of additional outlets on the pipeline.

Oromia Interrnational Bank (OIB): was established on September 2008 with authorized capital of Birr 1.5 billion, subscribed capital Birr 279.2 million and its paid-up capital was birr 91.2 million. OIB began its operation on October 25, 2008 by opening its first branch at the Dembel City Center. More specifically, its branch was named Bole Branch.

Zemen Bank: was established in 2009 in accordance with the commercial code of Ethiopia's 1960, its headquarter is located around Kazanchis Addis Ababa.

3.3. Data Collection

Since the study focuses on assessing the practices and challenges of ISP in Ethiopian banks the target population is the one which is directly related to the subject matter. Which are information security professionals, risk analysis and auditing team and the top management. Therefore the study is aimed at those key informants who will be appointed by the top management for the interview. Thus interviewees are selected by higher officials to serve a specific purpose.

The researcher conducted an informal minor survey (which is interviewing employees of different banks) before doing the actual research, this leads the researcher to conduct on interview data collection method only since there is no awareness about information security policy by the employees; so the researcher is forced to conduct the

research with respect to the opinions of information security professionals and, IT risk analysis and auditing professionals or the top managements. Based on the preliminary and [27] study revealed that the information security awareness in the banking sector in Ethiopia is unsatisfactory.

Primary data source is employed for the study. The interview data is collected through voice recording and taking notes simultaneously. The experience of the researcher with respect to the subject matter is also serves as a primary data.

3.4. Data Analysis

Data analysis involves critical thinking which is done after collecting the data from the respondents. Thus, the analysis of the study follows the objective of the research. The data from interviews is presented qualitatively in the discussion section. The data analysis is with respect to different standard principles.

Chapter 4 Data Presentation, Analysis and Discussion

In this chapter the raw data collected through interview are organized, tallied and structured so as to make it manageable for presentation and analysis. The interview has seven major questions. And hence all the findings presented below are summarized from these seven interview questions. The information obtained from key official informants from each selected banks and the researcher's personal observations are presented through narrative description. In addition, data presentation is done using table to present the summary of the collected data.

The structured in-depth interviews were carried out with the key personnel responsible for information security of the selected banks. In order to keep the privacy of the respondent's organizations, each ten bank is given a code that differentiates one another which is Bank 01 - Bank 10, instead of their actual identity and name of the organization; NBE is the only central bank of Ethiopia as a result there no need to give it a code. When conducting the interview, voice recording and not taking

4.1. Current Information Security and ISP practices in Ethiopian Banks

4.1.1. Bank 01

This bank has an Information Security team which is located under IT systems and infrastructure; it is not yet in department level, it is just a team located under department. The IT security team has 6 members, and each members of the team are not assigned to a specific role, they are all working in every aspects of information security domain. There are no standards or best practices to be followed by the given bank.

The bank has a formal documented information security policy, which comprises of different sub topics, it is only formulated by the IT security team, it is approved and

signed by the top management committee (Executives), all the policies are available to all employees but not implemented in all business units, the polices are easily understood by the users, its update is on 2 years interval, policies are distributed through all managers of business units then distributed to employees under each business units. As per the respondent it can be said that all policies and procedures are implemented and enforced.

All employees in the organization are forced to sign a confidentiality agreement or NDA. The organization had taken some disciplinary actions on employees who violate the policies and procedures for example, the organization has fired 3 employees until now, and some employees are under investigation. The organization does not provide any regular awareness program on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Complexity of information security domain: managements think that this domain is not that much complex and big.
- Lack of awareness: Employee's awareness regarding information security domain and IT in general is less.
- Lack of man power in the country: there is no special education for information security in the country. As a result hiring a professional is one of the challenges the bank faces.

Bank 01 is a member of PSS in the country, all members of PSS should follow the PCI DSS standard requirements. So this bank has implemented all the PCI DSS requirements.

The security team has planned to upgrade the information security team to department level, which can stand by itself, which can decide its financial budgets and the like. Currently management awareness is on a better progress. The team also has planned to make a better information security awareness program within the company that is supported by best industry practices in the world.

4.1.2. Bank 02

This bank does not have an Information Security department/team, but it has two officers working on information security domain in general, who work under infrastructure and applications team, and system development and customization team each. There are no standards or best practices to be followed by the bank.

This bank has a well-documented ISP by addressing important information security topics, which they have not found anything in their day-to-day life which is not covered by it, as per the respondent it is a complete policy. IT security officers are the only members of the committee who formulates the policy. Approval of the policy is done by executives committee; all the policies are partially available to everyone through distributing to each business units and branches of the bank. As per the respondent it can be said that all policies are understood by everyone.

This bank reviews their information security policy once a year as a practice, but if there is an urgent incident there might exist an immediate review of the policy.

A few employees who work on organizations critical information assets are forced to sign a confidentiality agreement or NDA. The organization does not provide any regular awareness program on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Lack of good security culture in the organization.
- Lack of employees as well as managements awareness
- Lack of man power in the country: there is no special education for information security in the country as a result hiring a professional is one of the challenges the company faces.
- Lack of industry standard or best practice locally

Currently this bank is running a big project to design and develop information security management system (ISMS).In the future awareness, policy enforcement, risk management and the like team will be formed.

4.1.3. Bank 03

This bank has an Information Security department, which is located under vice president of IT. The IT security department has 2 members, and each members of the team are not assigned to a specific role, they all working in every aspects of information security domain. There are no standards or best practices to be followed by the given bank.

This bank has a well-documented ISP by addressing important information security topics. IT security officers are the only members of the committee who formulates the policy. Executives committees are the one who approves and sign the policy, all the policies are partially available to everyone through distributing to each business units and branches of the bank. It can't be said that all policies are understood by everyone. The policies are reviewed and updated every year.

Only a few employees in the organization are forced to sign a confidentiality agreement or NDA. The organization does not provide any regular awareness program on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Lack of procedures and guidelines, policies cannot be applicable without the presence of a well written procedures and guidelines that support the policies.
- Lack of awareness: Employee's awareness regarding information security domain and IT in general is less.
- Lack of man power in the country: there is no special education for information security in the country as a result hiring a professional is one of the challenges the company faces.

In the future the security team has planned to be directly under the president since there are some confidential information that must only be seen by the president who is responsible for it.

4.1.4. Bank 04

This bank has an Information Security team which is not in department level, it has three officers working on information security domain in general, which works under vice president of Systems and e-banking. Information security governance is directly lead by the board (executives committee).COBIT serves as an information security governance framework for the organization.

The bank has a formal documented information security policy, which comprises of different sub topics, as per different standards it is formulated by committees from different business units, it is approved and signed by the top management committee (Executives), all the policies are partially available to employees, it cannot be said that polices are easily understood by the users, policies are distributed through all managers of business units then distributed to employees under each business units. The bank reviews its policy once a year as a practice, but if there is an urgent incident there might exist an immediate review of the policy.

All employees in the organization should sign a confidentiality agreement or NDA. The organization has taken series disciplinary measures on employees. The organization does not provide any regular awareness session for employees on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Lack of employees as well as managements awareness
- Lack of specialized man power in the country
- Lack of industry standard or best practice locally

Managements have reached on a consensus to follow industry's best practices and standards and to give a higher support and commitment for information security domain.

4.1.5. Bank 05

This bank has an Information Security department, which is located under vice president of IT services. The IT security department has 2officer, and each members of the team are not assigned to a specific role, they all working in every aspects of information security domain. There are no standards or best practices to be followed by the given bank.

The bank has a formal documented ISP, which comprises of different sub topics, as per different standards it is formulated by committees from different business units, it will be approved and signed by the top management committee (Executives), all the policies are not available to anyone yet, policies will be distributed through awareness trainings and through copy of each policy to all managers of business units then distributed to employees under each business units. The bank planed to review its policy once a year as a practice, but if there is an urgent incident there might exist an immediate review of the policy.

Only a few employees in the organization are forced to sign a confidentiality agreement or NDA. The does not take any disciplinary actions yet.

The company faces the following challenges in formulation, implementation and compliance.

- Management's commitment is less: it's been a year since the policy is drafted, but it is in the hands of management for approval purpose.
- Lack of awareness: Employee's awareness regarding information security domain and IT in general is less.
- Lack of standard and best practices in the country.

The future plan is not yet set by the top managements, the policy is expected to be approved by the executives.

4.1.6. Bank 06

This bank does not have an Information Security department or team, there is only one information security personnel which takes orders directly to the CIO. It's been three months since the officer is hired, so there is no that much work he has done. The bank does not follow any specific standard or best practice.

The bank has a well-documented ISP, which comprises of different sub topics, as per different standards it is formulated by committees from different business units, it is approved and signed by the top management committee (Executives), it has been three years since the policy is developed and approved, it is not yet available to all employees, it cannot be said that polices are easily understood by the users, none of the policies are implemented and enforced. The bank reviews its policy once a year as a practice, but if there is an urgent incident there might exist an immediate review of the policy. IT innovation and system engineering team is the one who developed and formulated the policy and they are responsible for reviewing and updating the policy too.

All employees in the organization should sign a confidentiality agreement or NDA. The organization has not taken any disciplinary measures yet on employees. The organization does not provide any regular awareness session for employees on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Lack of employees as well as managements awareness on information security
- Lack of specialized man power in the country
- Lack of industry standard or best practice locally

Managements have reached on a consensus to follow industry's best practices and standards and to give a higher support and commitment for information security domain and they have also decided to reformulate the policy.

4.1.7. Bank 07

This bank has an Information Security team which is not in department level, which is located under department manager of IT. The IT security division has 3 officer, and each members of the team are not assigned to a specific role, they all working in every aspects of information security domain. There are no standards or best practices to be followed by the given bank.

The bank has a formal documented ISP, which comprises of different sub topics which are around 40 policies and 13 procedures, it is formulated and developed by systems security division and then commented by various business units, it was approved and signed by the board (Executives), all the policies are available to everyone in the organization and it is distributed through hard copies, softcopies and the organizations internal portal. The bank has planned to review its policy every 2 year as a practice..

Everyone in the organization should sign on a confidentiality agreement on organizational policy at their hiring process, then after the hiring process when they are assigned on a specific duty they should sign on a document to confirm that they read some specific policies. The organization does not take any disciplinary actions yet on those that violates the policies. There is no regular awareness program taken by the bank.

The company faces the following challenges in formulation, implementation and compliance.

- Managements give less attention to the subject due to less awareness
- Lack of a good security culture
- Lack of standard in the country

The organization has a project that is on a progress, which is conducted by an international company called Ernst and Young to investigate the company's overall systems/processes and the organizations' security.

4.1.8. Bank 08

This bank has an Information Security department/team, it has 30 officers working on information security domain in general, and the department is under vice president of chief and risk compliance. There has been a project taken by other company for development of a new structure and system for information security management system based on various standards like ISO, NIST and SANS but the bank has not started yet implementing this new structure and system.

This bank has a well-documented ISP by addressing important information security topics, but it has not yet signed and approved by the top managements or executives. Consultants from other company are the one who mainly formulates the policies and information security officers from the bank participates in the formulation. The policies does not reach to employees since it is not yet approved and signed. The bank has planned to review the policy on yearly basis.

A few employees who works on organizations critical information assets are forced to sign a confidentiality agreement or NDA. The organization does not provide any regular awareness program on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Management's commitment to information security domain is less, it has been 2 years since the policy is developed and drafted but it is still not been approved. It might be due to lack of managements awareness.
- Lack of man power in the country: there is no special education for information security in the country as a result hiring a professional is one of the challenges the company faces.

- Lack of good security culture in the organization.
- Lack of industry standard or best practice within the country.

4.1.9. Bank 09

This bank has an Information Security management office, there are three officers working under it, they are highly paid staffs from all the business units in the organization since management believe that they are the key personnel's in organization. The security management office takes direct orders from the vice president of IT. There is no specific role assigned to the officers yet. The bank follows ITL standards for information security governance as a best practice.

The bank has a well-documented ISP, which comprises of different sub topics, as per different standards it is formulated by committees from different business units and consultants from Kenya who has a good experience in the field, it is approved and signed by the top management committee (Executives), it has been three years since the policy is developed and approved, it is distributed to all employees through exchange servers and by pushing on their desktop by Active Directory, as per the interviewee it can be said thatall polices are easily understood by the users. The bank reviews its policy every 2 year as a practice, but if there is an urgent incident there might exist an immediate review of the policy. Each business unit managers and employees, information security team and all Executives are responsible for reviewing and updating he policy.

All employees in the organization should sign a confidentiality agreement or NDA. The organization has not taken any disciplinary measures yet on employees. The organization does not provide any regular awareness session for employees on information security domain.

The company faces the following challenges in formulation, implementation and compliance.

- Lack of employees as well as managements awareness on information security
- Lack of specialized man power in the country
- Lack of industry standard or best practice locally, there is no industry bench marks in the country

The organization is moving towards new technological advancements like mobile banking, e-payment etc… as a result of this, threats to the organization will rise, so to mitigate this risks managements planned to have a higher security mechanisms.

4.1.10. Bank 10

This bank has an Information Security department, which is located under vice president of IT in Information security section. The IT security section has 2officers, and each members of the team are not assigned to a specific role, they all working in every aspects of information security domain. There are no standards or best practices to be followed by the given bank.

The bank has a formal documented ISP, which comprises of different sub topics, the banks' ISP is formulated and developed by an international organization from outside of Ethiopia before 3 years, it was approved and signed by the top management committee (Executives), all the policies are not available to anyone yet, policies. Currently the ISP is maintained and reviewed by the IT security section and the team also reviewed once since it's' development. The bank planned to review its policy once a year as a practice, but if there is an urgent incident there might exist an immediate review of the policy.

Only a few employees in the organization are forced to sign a confidentiality agreement or NDA. The bank had not taken any disciplinary actions yet.

The company faces the following challenges in formulation, implementation and compliance.

- Information Security man power in the bank as well as in the country

- Lack of procedures, procedures are not yet formulated and implemented.
- Lack of a good security culture
- Lack of standard in the country

4.1.11. NBE

NBE has an Information Security department which is newly formed and it is under vice governor of corporate. There are two officers working under information security department. It's been four months since the department formed, so there is no that much work the department has done. The bank does not follow any specific standard or best practice.

NBE has a well-documented ISP, which comprises of different sub topics, as per different standards it is formulated by another organization and members of IT department, it is approved and signed by the top management committee (Executives), it has been a year and half since the policy is developed and formulated, it is not yet available to all employees, it cannot be said that polices are easily understood by the users, none of the policies are implemented except password usage policy which is implemented and enforced through active directory. The bank reviews its policy once a year as a practice, but if there is an urgent incident there might exist an immediate review of the policy. IT innovation and system engineering team is the one who developed and formulated the policy and they are responsible for reviewing and updating the policy too.

All employees of NBE do not sign any confidentiality agreement or NDA. The bank has not taken any disciplinary measures yet on employees. The organization does not provide any regular awareness session for employees on information security domain.

NBE faces the following challenges in formulation, implementation and compliance.

- Lack of employees as well as managements awareness on information security
- Lack of specialized man power in the country
- Lack of industry standard or best practice locally

NBE is the regulatory body in any Ethiopian financial sector under the Proclamation of Federal Democratic Republic of Ethiopia No. 592/2008 on Federal Negarit Gazeta, which is responsible for the supervision of the following information security related issues in financial institutions.

- Assess whether Ethiopian banks have a disaster recovery site for their data center.
- Assess whether Ethiopian banks have installed Antivirus on their information system components.
- Assess whether there is a central directory services to authenticate users
- Assess whether there is an information security personnel in the bank
- Assesses their IT audit reports
- Assess their fraud registries or logs. All microfinance institutions shall have a well-written monitoring and control policies, approved by the Board, and procedures for fraud detection, mitigation and reporting as stated in the Licensing and supervision of the business of microfinance institutions Fraud Monitoring Directives No. MFI/26/2014.

Any bank that fails to comply with the requirements of any of the directives of National Bank of Ethiopia, shall be subject to a penalty of birr 10,000 (ten thousand birr) for each violation.

NBE is running a big project with INSA (Information Network Security Agency) to develop Cyber Security Framework for Ethiopian Banking Industry with the initiative of NBE.

4.2. Summary of Information Security and ISP Practices

No.	Description	Banks										
		01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**NBE**
1.	Is there Security Department	Yes, but not in department level	No, But there are information security officers working on information security	Yes	Yes, but now in department level yet	Yes	Yes, not in department level	Yes, not in department level	Yes	Yes, but it is in team level	Yes	Yes
	• How many employees under it?	6	2	2	3	3	1	3	30	3	2	2

	• Is there a dedicated personnel for security awareness, policy enforcement, risk management?	No	No	No	No	No	No	No	No	No	No	No
	• Is there any standard to be followed?	There is no specific standard	There is no specific standard	There is no specific standard	Yes, COBIT for information security governance	There is no specific standard	There is no standard to be followed by the organization	There is no standard to be followed by the organization	There is no specific standard	There is no specific standard	There is no specific standard	There is no specific standard
2.	Is there a formal documented Information Security Policy?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	• Which leadership level approves it	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board	Executives/Board
	• Are all the polices implemented and enforced?	Yes	Partially	Partially	Partially	Few	None	Yes	No, it's on approval stage	Yes	Few	No
	• Is there an owner to maintain and review?	Yes, IT Security team	Not yet	Yes, it is the security team	Yes, security team is responsible	Yes, security team	Yes, IT innovation and System engineering team is responsible	Yes, IT department is responsible for maintaining, updating and reviewing the policy	Not yet, but it is considered to be IS compliance team	Yes, each business units are considered as owners	Yes, security office and IT management	Yes, security team

	• Is it available to everyone ?	Yes	Partially	Not yet	Not yet	Not yet	Not yet	Yes	Not yet	Yes	Not yet	Not yet
	• How is it distributed?	To all managers then to employees	Hard copy to each business units and branches	Hard copy to each business units and branches	Hard copy to each business units and branches	Not distributed yet	It is distributed to branches only	It is distributed through Hard copies, soft copies and the organizations' internal portal	Will be distributed using portal	Using awareness training and copy the document in to each PC	Will be distributed using hard copy of the policy	
	• Is it easily understood?	Yes	Yes	Can't be determined	Can't be determined	Can't be determined	Yes	Yes	Can't be determined	Yes	Can't be determined	
	• How frequently it is updated?	Yearly	Yearly	Yearly	2 years	Yearly	Yearly	Every 2 year	Yearly	2 years	Yearly	

	• Who participate in formulation?	Only IT Security Team members	Only IT security officers	Only IT security officers	Different business units	Only IT security officers	Only IT innovation and system engineering team members only	Only IT department members and information security officers	Third party consultant and IT security officers	Consultants from Kenya and all business unit members	Consultants and IT security officers	
4.	Do all employees sign NDA?	Yes	Few	Few	Yes	Few	Yes	Yes	Some	Few	Few	No
5.	Does the organization take any disciplinary actions?	Yes	No	Yes	Yes	No	No	No	No	Yes	Yes	No
6.	Does the organization organize regular information security awareness program?	No	No	No	No	No	No	No	No	No	No	No

7.	Challenges in formulation, implementation and users compliance?	• Complexity • Lack of awareness • Lack of man power in the country	• Lack of man power in the country • Lack of good security culture • Lack of standard in the country	• Lack of procedures • Lack of man power • Lack of standard in the country	• Lack of man power • Lack of standard in the country • Lack of managements awareness and commitment	• Lack of information security awareness • Managements less emphasis on subject matter • Lack of standard	• Lack of man power • Lack of standard in the country • Lack of managements awareness and commitment	• Less management awareness on the field • Lack of standard to meet	• Lack of standard in the country • Lack of management's commitment and support	• Change management resistance • Lack of man power in the countr y	• Continuous change of rules and regulations • No clear NBE standard to meet • Industry best practices does not exist	• Lack of managements support and commitment • Lack of procedures
8.	Which of the following polices have you implemented ?											

	• Access Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Acceptable Usage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Information Handling	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓
	• Network Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Personnel Security	✓	✓	✓	✓	X	✓	✓	✓	X	✓	✓
	• Password Usage	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
	• Internet Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• E-mail Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Encryption	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓

	• Malicious Software Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Backup and Restoration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Hardware and Software Acquisition, Development and Maintenance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	• Data center security	✓	✓	✓	✓	X	✓	X	✓	✓	✓	✓
	• Physical and environmental security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	• Incident management	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓
	• Change management	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓

Table 3: Information Security and ISP practices in Ethiopian banks

4.3. Discussions

- **How is the current practice of Information security in Ethiopian Banks?**

The world is now moved on to third generation of information security which is taking human element into consideration, when we come to our country we can say that we are still on the second generation of information security which is finding best practices and processes for governing information security.

In almost all banks, management does not give that much emphasis to information security, for implementing a good and effective information security governance management commitment and support is highly mandatory. Most of the banks management has less awareness on information security issues. Information security departments are not that much organized and in a proper structure (information security department should be directly lead by the president or the board).

Almost all banks do not follow a specific standard or best practice for the information security governance. All banks except two banks (bank 01 and 08) have less than 4 information security officers, and no one is dedicated for a specific role in each bank.

- **How is the current practices of ISP in Ethiopian Banks?**

The empirical findings as shown above revealed that the current practices of ISP can be said that it is in its infant stage, since only three banks (bank 01, bank 07 and bank 09) in Ethiopia implements and enforces ISP partially in the organization, but the rest of the banks does not even implement it well.

Most of the banks formulate and develop ISP because of the regulatory body orders them to do so, but they must develop and formulate ISP based on their initiations by understanding its' importance. ISP is one of the mandatory components of any information security program.

Most of the organizations ISPs' are formulated by information security office only, this makes it hard to implement since information security officers is not aware about exact requirements of each business units and not much aware about any regulatory legislations.

The security team is the owner of ISP in all banks except bank 09. But according to different standards and best practices the owner of ISP should be the top management, each business unit's managers, and information security office.

Five out of eleven banks have taken some disciplinary actions on those that violate the bank's ISP.

Developing and having an ISP does not solve security problems without having frequent checkup and frequent update.

It can be said that all banks addresses most relevant policies in their ISP and each policy addresses the objectives of policy; legislative, regulatory, and contractual compliance; and penalties for non-compliance with the organizations policies.

- **What are the challenges in formulating, implementing and compliance of ISP in Ethiopian Banks?**

As it was revealed from the interview and the researchers' observation, there are some challenges that each organizations or banks face during the formulation, implementation and compliance of ISP. Some of the challenges that are faced are listed below:

- Management's commitment and support due to lack of awareness is one of the biggest challenges each banks faces.
- Lack of a special training to information security personnel's. Management becomes afraid of providing the proper training to network security professionals because they thought that the employee that took the training will just leave the company and use the skills for other competitor.

- Complexity of the subject matter, information security by its nature is very dynamic and complex. It is a very broad area to study.
- There is no specific education/curriculum in the country, hence hiring a professional is very unthinkable.
- The regulatory body which is NBE has not developed a standard that each bank in the country should follow. Lack of this standard is one of the problem Ethiopian banks faces.
- Tailoring international standards is one of the complex task
- There is a resistance with employees to comply with ISP's due to two reasons; the first reason is due to lack of awareness and the second reason is most of the policies does not fit some business units. As a result of these reasons most of the employees in the organizations find it hard to comply with the organizations ISP's.
- Lack ongoing personnel awareness on security issues. Every banks in the country does not have any regular awareness program for employees, so employees of the organization might be the cause for a threat.

- **What are the future prospects of ISP in Ethiopian Banks?**

Now a days some of the banks' management believe that ISP is one of the most mandatory component of any information security program, hence each organization have planned to review and update their ISP's and some of the organization planned to have an adequate Information security management system/process which incorporates having an adequate management structure for information security this can be achieved through giving training for information security officers, hiring a professionals on the area etc.

Chapter 5 Conclusion, Recommendations and Future Works

5.1. Conclusions

The purpose of this study is to understand what the practices of Information security and ISP, to investigate the challenges Ethiopian banking industry faces in formulating and implementing ISP and to investigate the future prospects regarding the field.

The study revealed that there is no as such common Information security governance standard within the banking industry of Ethiopia. In some cases the banks information security team may be under risk and compliance team, information technology innovation team, IT team etc. this shows that there is no consistency in governing information security. And also the study revealed that there is no adequate man power in any of Ethiopian banks information security team/office.

It is important that senior management is committed to supporting the information security initiative but in the case of our country's banking industry the initiative comes from the information security office only, this makes it hard to implement a good information security program.

All 11 respondents from each bank were asked the presence of a documented ISP that governs the information security, and they all responded that a documented ISP existed but their level of implementation differs. They all formulate and develop their policies because of the regulatory body orders them to devise their policies. A policy-writing team, commissioned by a management oversight committee, should construct the policy to reflect the corporate culture.

A good Information Security Awareness Program highlights the importance of information security and introduces the Information Security Policies and

Procedures in a simple yet effective way so that employees are able to understand the policies and are aware of the procedures.

Information security researchers have recently emphasized that management's attention is required to secure information resources to design effective security policies, and to enhance users' security awareness to comply with information security policies. People are recognized as the weakest link in the information security chain, but are considered abundant assets in the effort to reduce information security threats [6]. Therefore, ISPs must be designed to provide employees with guidelines on how to address the integrity, availability, and confidentiality of information resources they use in performing their jobs.

5.2. Recommendations

Senior management is responsible for: Establishing the organization's information security program; Setting program goals and priorities that support the mission of the organization; and making sure resources are available to support the information security program and make it successful.

User training is very important to succeed in any project. Because users should be aware what is actually happening and they should have a clear idea about their roles and responsibilities. In information security too, users' awareness is a very important aspect for the success of the project. This basically should be at the beginning whenever employee joins the organization (induction program) and in regular intervals or when there is a significant change in policies or procedures. And it is important to have easy access to policies and procedures they are enforced to practice.

Security awareness personnel's need to inform and educate the organizations' employees about its security policies and persuade the users to engage in secure computing practices. Business units and users must know that they are an integral part of the information systems security process. Employees should

be aware of what is actually happening and they should have a clear idea about their roles and responsibilities. The security awareness program basically should start at the beginning when an employee joins the organization using an induction program, then conducting a regular awareness program whenever there is a new thing regarding any information security issues.

The information security team must constantly struggle to improve the process and provide the best defense against any threats to the organization. Whenever there is a security breach, it should be treated as an important incident; the suspects should be identified and then trying to find a mitigation for it.

Many employees in an organization are exposed to the organizations information, to minimize disclosure of the organizations information assets to outsiders, it is necessary to make them aware about information security controls and necessary to make legal enforcements like signing confidentiality or non-disclosure agreements.

Here are some of the recommendations for implementing and enforcing ISPs'

- The top managements have to take international courses related to Information security; their level of awareness should be up to date. Managements are the one who is responsible for every action taken in the organization.
- Information security leader should have autonomous decision
- Having a complete set of documented security policies should not be viewed as optional for any business.
- Keeping the policies updated is the important thing that must be done. So banks should have to update their policies with regular period of time.
- Banks should only document the policies that they intend to enforce, unless there is no need for formulating or developing the policy.

- Banks have to make sure that every employee has access to the policies, reads the policies, and acknowledges that they will abide by the policies.
- Banks have to include policy awareness/education as a part of ongoing security awareness training for all organizations employees.
- Banks have to identify and use mechanisms that help them to determine if their policies are complete, are understood, and are being followed.

5.3. Future Works

The research helps assess information security and ISP practices, and to investigate the challenges and prospects in the process of formulation and implementation of ISPs within the Ethiopian banking industry. As a result of this, the study helps to have the following researches to be conducted:

- Assessing the impact of following a specific standard
- Formulating a standard information security policy in Ethiopia's banking industry
- To further investigate the challenges in each specific policies of the banks
- Assessing why banks people less aware of ISP

References

[1] Herath T. and Rao H. R (2009), "*A framework for security policy compliance in organizations*," European Journal of Information Systems.

[2] AleksandarKlai (2011). "*Methods and Tools for the Development of Information Security Policy: A Comparative Literature Review*". Croatia Office of National Security Council.

[3] Mahncke, R. J., McDermid D. C.& Williams P.A. (2009). "*Measuring Information SecurityGovernance within General MedicalPractice*," Proceedings of the 7th AustralianInformation Security ManagementConference, Australia.

[4] Kelemie T., (2013). "*Information Security Management Framework for Bank industry in Ethiopia*", Addis Ababa University, Ethiopia.

[5] Mark R.Ousley, (2013). "*Complete Reference: Information Security*". 2nd edition, McGraw, USA.

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

[7] Haag, S., & Cummings, M. (2008). "*Management information systems for the information age*". New York, USA: McGraw Hill.

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

[9] ISO/IEC 27001:2009. "*Information technology – Security techniques – Information security management systems – Overview and Vocabulary*".https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

[10] Powell, T. C. and Dent-Micallef, A. (1997). "*Information Technology as competitive advantage: the role of human, business, and technology resources*". Strategic Management journal. USA.

[11] Bulgurcu B., Cavusoglu H., and Benbasat I., (2010) "*Information security policy compliance: an empirical study of rationality based beliefs and information security awareness*," Turkey.

[12] Whitman M., Townsend A., and Aalberts R., (2001). "*Information systems security and the need for policyin Information Security Management".*Idea Group Publishing, USA.

[13] Siponen M., Pahnila S., and Mahmood A., (2007)."*Employees' adherence to information security policies: an empirical study*" in IFIP International Federation for Information Processing, Springer, USA.

[14] Munirul U., Zuraini B.,&Zailani M., (2011). "*A Framework for the Governance of Information Security in Banking System*".IBIMA Publishing.UniversitasMalikussaleh. Indonesia.

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

[16] Solomon, M and Chapple, M. (2005). "*Information Security Illuminated*". Jones, and Bartlett Publishers.

[17] Byrnes, Christian F., and Dale Kutnick (2002). "*Securing Business Information: Strategies to Protectthe Enterprise and Its Network*". Addison Wesley.

[18] Michael E. Whitman, Herbert J.Mattord,(2012) " *Principles of Information Security*", Kennesaw State University. 4th Edition.

[19] Tudor, Jan K. (2006)."*Information Security Architecture: An Integrated Approach to Security in theOrganization*". CRC Press.

[20] Maiwald, E and Sieglein, W. (2002). "*Security Planning & Disaster Recovery*".Berkeley, McGraw-Hill/Osborne.

[21] Liu S, Sullivan J.Ormaner J. (2001) "*A Practical Approach to Enterprise IT Security*". IEEE IT Professional.

[22] Hamill JT, Deckro RF, Kloeber-Jr. JM (2005) "*Evaluating Information Assurance Strategies. Decision SupportSystems*"

[23] McCumber, John (2004). "*Assessing and Managing Security Risk in IT Systems: A StructuredMethodology*". Auerbach Publications.

[24] Atif Ahmed, Sean B.Maynard, Sangseo Park (2012). "*Information Security Strategies: Towards an Organizational Multi-Strategy Perspective*".Melbourne School of Engineering.

[25] Alexander Ilic, Trevor Burbridge, Andreas Soppera, Florian Michahelles, (2007). "*A threat model analysis of EPC based Information sharing networks*".

[26] Mahi Dontamestti, AnupNarayannan, (2009). "*Impact of the Human Element on Information Security*".Information Science Reference, New York, USA.

[27] AbiyWoretaw and Lemma Lessa (2012)."*Information Security Culture in the Banking in Ethiopia*".5th ICT Ethiopia Conference.

[28] Ayana Gemechu (2014). "*Factors Affecting Adoption of Electronic Banking System in Ethiopian Industry*".Ambo University, Journal of Management and Information System and E-commerce.

[29] Thomas R. Peltier and Justine Peltier (2007). "*A Complete Guide to CISM Certification*".Auerbach Publications, USA.

[30] Harold F.Tipton, Micki Krause (2007). "*Information Security Management Handbook: Information Security Governane*". Auerbach Publications, USA. 6thed.

[31] PCI DSS (2013)
"*https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf*" Version 3.0.

[32] COBIT 5(2012). "*http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf* "

[33] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14, "*Generally Accepted Principles and Practices for Securing Information Technology Systems*"

[34]Moulton, R & Coles, R. S. (2003). "*Computers and Security: Applying Information Security Governance*" Elsevier Publisher.

[35] Harris S. (2006)."*Information Security Governance Guide*".

[36] Peter Gregory (2003). "*Enterprise Information Security: Security for Non-technical Decision Makers*". Pearson Education.

[37] MuraliKrisha (2010). "*A Methodology for Measuring Information Security Maturity in Norweigian and Indian MSME's with Special Focus on People Factor*". Gjovik University.

[38] Kerry D.McConnel (2013). " *How to Develop Good Security Policies and Tips on Assessment and enforcement*" SANS Institute, USA.

[39] Neil R.Doherty, Heather Fulford. (2009). "*Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis*". Loughborough University, UK.

[40] UCISA (Universities and Colleges Information Systems Association), (2005). "*Information Security*".Information Press, UK.

[41] Sushma Mishra and Gurpreet Dhillon (2008). "*Information System Security Governance Research: A Behavioral Perspective*". Virginia Common Wealth University, USA.

[42] SANS (2002). " *A Preparation Guide to Information Security Policy"*. SANS Institute.

[43] Thomas R. Peltier, (2004). "*Information Security Policies and Procedures*".Auerbach Publications, New York.2nd Ed.

[44]SANS (2009). "*How to Establish a Security Awareness Program*".SANS Institute.

[45] Dutta A. and McCrohan R. (2002)."*Management's Role in Information Security in a Cyber economy*," California Management Review, USA.

[46] KragBrotby W. (2009) " *Information Security Governance: Guidance for Information Security Managers*" IT Governance Institute (ITGI). USA. www.itgi.org

[47] Alexander I. Trevor B, Andrea S. Florian M (2007). " *A Threat Model Analysis of EPC-base Information Sharing Networks*".

[48] SANS (2001). " *Introduction and Education of Information Security Policies to Employees in My Organization*". SANS Institute.

[49] B.A.R.L Jayawardana (2011). " *Information Security Challenges in Relation to Enterprise Security Policies in the Financial Sector in Srilanka*". University of Colombo, Srilanka.

[50] Ayichiluhim D. (2013). " *Internet Banking Security Framework: the Case of Ethiopian Banking*". HiLCoE Ethiopia.

[51] Behabtu A. (2015). " *Assessment of Insider Threat in Ethiopian Banking Industry*". Addis Ababa University, Ethiopia.

Appendix A:Outline of the Interview

1. Do you have Information Security Department?

   If you have

   a. Where is it located in the structure of the organization?
   b. Which information security governance standard do they follow?
   c. How many employees under it?
   d. Do you have information Security Staff Dedicated to
      i. Security Awareness
      ii. Policy Enforcement
      iii. Risk Management

      - Management must set direction and provide support for information security. The purpose of this question is to assess top managements attitude regarding information security, with trying to see how much emphasis they give in building the department (how much managements are committed and support the information security), if they give a higher emphasis on the issue they would hire a specialized workforce under the department, which standards they follow in information security governance and to assess whether they assign a dedicated personnel in security awareness, policy enforcement, risk management etc.

2. Do you have documented Information Security Policy?

   - Helps to assess whether there is a formal documented ISP or not?

   If you have

   a. Which leadership level approves the ISP's?

- ❖ For an information security to be implemented effectively a higher officials should approve, sign and give direction to be implemented in all the organizations business units.

b. Are all the policies implemented and enforced?

- ❖ Helps to assess whether ISP is implemented and enforced or not in the organization. If it is implemented to investigate what are the strengths and what are the weaknesses.

c. Is there an owner to maintain and review the policies?

- ❖ For an ISP to be implemented there must be someone who maintains and review all the policies in the organization.

d. Are all the polices available to everyone?

- ❖ An ISP is effective when everyone in the organization is aware of it, without awareness of employees it is hard to the organization to implement and enforce ISP.

e. How does the ISP's communicated to employees?

- ❖ To assess whether it is a good mechanism to distribute to all the employees.

f. Who participate in the formulation of the ISP's?

- ❖ Effective ISP should be formulated from different department member not only Information security department.

g. Are all the policies easily understood by everyone?

- ❖ To assess whether the policy is easily understandable by the employees of the given organization, if it is not easily understandable it hard to implement and enforce the ISP.

h. How frequently polices are updated?

- ❖ Every policies should have a time period to update and maintain it to ensure that policies remain appropriate in any relevant changes to the law, organizational policies or contractual obligations.

If you don't

i. How is your procedural (Traditional) work?

- ❖ Helps to assess how the current information security practice in the organization related to ISP.

3. Do all employees sign a confidentiality agreement/NDA?

- ❖ Employees of the organization may have a valuable information, so to minimize information disclosure to outsiders, employees should be aware of the information security control and they will sign that they are going to be abide by the agreement/law. So this question tries to see whether there is an NDA or not between the organization and the employee.

4. Does your organization take any disciplinary actions against employees who violate ISPs'?

    - ❖ To assess whether there is any disciplinary measures taken by the organization. Since this disciplinary action taken should be taken as an example for others.

5. Does your organization organizes regular awareness programs for educating employees on ISP's, Procedures and guidelines?

    - ❖ Any employees in the organization should be aware of the policies, procedures, guidelines and even up to date information security issues. So this question helps to assess whether there is a regular information security awareness session or not.

6. What are the challenges that you face in formulation, implementation and users compliance of ISP's?

    - ❖ To assess the challenges that the organization faces in the formulation, implementation and users compliance of ISP's.

7. What is your future plan regarding ISP?

    - ❖ Helps to assess what the organization plan to do in the future regarding information security or ISP.

8. Thick the policies that your ISP have
    - ❖ The intent of this question is to assess whether the organizations ISP address the following relevant policies.

	ISP's	YES	NO
1.	Access Management Policy		
2.	Acceptable Usage Policy		
3.	Data/Information handling Policy		
4.	Network Security Policy		
5.	Internet Security Policy		
6.	E-mail Security Policy		
7.	Personnel Security Policy		
8.	Password usage policy		
9.	Encryption Policy		
10.	Malicious Software Protection Policy		
11.	Backup and Restoration Policy		
12.	Hardware and Software Acquisition, Development and Maintenance Policy		
13.	Data Center Security Policy		
14.	Physical and environmental Security Policy		
15.	Incident Management Policy		
16.	Change Management Policy		

Table 4: Some common ISP's

Do the ISP's contain the following topics?

- ✓ Objectives of the policies? Yes [ ] No [ ]
  - ❖ Objectives of policies should be stated in order to be meet the objectives or goals of the policy. So this question helps to check whether there is a clear objective set in each policies.

- ✓ Legislative, regulatory, and contractual compliance requirements? Yes [ ] No [ ]

- ❖ The purpose of this question is to assess whether there is legislative, regulatory and contractual compliance requirements to meet.

✓ Penalties for non-compliance with corporate policies? Yes [ ] No [ ]

- ❖ The purpose of this question is to assess whether there exists a penalty or not when violating the given policy.