ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

MATURITY OF INFORMATION SYSTEMS SECURITY IN SELECTED PRIVATE BANKS IN ETHIOPIA

By

TADELE SHIMELS

JUNE, 2021
ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

MATURITY OF INFORMATION SYSTEMS SECURITY IN SELECTED PRIVATE BANKS IN ETHIOPIA

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

By: TADELE SHIMELS

Advisor: LEMMA LESSA (Ph.D.)

June, 2021

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE
SCHOOL OF INFORMATION SCIENCE

MATURITY OF INFORMATION SYSTEMS SECURITY IN SELECTED PRIVATE BANKS IN ETHIOPIA

By: Tadele Shimels

Name and signature of Members of the Examining Board

Lemma Lessa (Ph.D.) Advisor	_____ Signature	_____ Date
Getachew Hailemariam (Ph.D.) Examiner	_____ Signature	_____ Date
Temtim Assefa (Ph.D.) Examiner	_____ Signature	_____ Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university. I declare that this thesis entitled "***Maturity of Information Systems Security in Selected Private Banks in Ethiopia***" this research is the outcome of my own investigation. I conducted the research on my own, with the encouragement and assistance of my research advisor. Other sources are accepted by citations that include clear references. A list of references is included at the end.

Signature: _____

Tadele Shimels

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

Advisor's Signature: _____

Lemma Lessa (Ph.D.)

Acknowledgements

First and foremost, I want to express my gratitude to the almighty GOD for providing me the strength, courage, wisdom, and persistence necessary to complete this research.

Dr. Lemma Lessa, my advisor, has provided me excellent support. Working under the guidance of such an academic man has been a blessing! Thank you very much, Dr. Lemma, for your insightful advice, motivation, and encouragement, as well as your patience for my weaknesses. You were on time, courteous, and supportive in sharing all of the helpful tools you have with your students. May God reward you for your unforgettably inspiring efforts to help your students!

My sincere thanks also go to all of my instructors at the school of information science, as well as all of the research participants from different banks!

I'd like to express my sincere gratitude to the banks for allowing me to conduct my study, and I consider the CIO, Directors, and Managers of the sampled private banks in great respect for their assistance during data gathering. Haimanot Gezahegn and Mahlet Habtamu for their kindness and attention during my years of study, as well as during the analysis and writing of this thesis.

Special thanks to **Bitanya Tadele, my daughter!!!**

Abstract

This research examines the Ethiopian private banking industry's information system security maturity level. The study aims to assess the current maturity level and examine the difference in order to make potential improvements. Protecting information system security and minimizing security concerns is more critical than ever before. The banking industry has put investment into the economy in order to help it grow. Despite their critical position in the economy, banks are still vulnerable to failure. Banks, like any other IT infrastructure, could go bankrupt. Unlike any other business entities, though, their failure would have a significant effect on their clients, suppliers, and shareholders, as well as the country's economic stability.

This study was carried out using questionnaire survey data collection. As well as the review of documentation and information security policy and guidelines, were performed. The researcher selects four private banks as a sample and distributes a questionnaire. The measurement has conducted based on ISO/IEC 27001, an internationally accepted information security standard.

The data obtained from the questionnaire is analysed using descriptive data analysis, and SPSS is used to interpret and present the data. This study assesses the current maturity level of Ethiopia's private banking sector, as well as the strength and weakness of information security maturity level control objectives based on ISO 27001's fourteen security areas. The report also discusses possible improvements that should be implemented in order to achieve the maximum degree of information security maturity.

According to the findings of the study, the private banking industry's current maturity level is 2 (repeatable but intuitive). The report helps for a better understanding of information security concerns and recommends for Ethiopian private banks to utilize information security management as a strategically significant component. The findings of the study could also be used by these banks to rearrange their information security management systems.

Keywords: *Information Systems Security, Information Systems threat, Information Systems Security maturity*

Table of Contents

List of Tables

List of Figures

List of Acronyms

ATM	Automated Teller Machine
BSI	British Standard Institution
CIA	Confidentiality, Integrity and Availability
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and Related Technologies
CMDB	Configuration Management Database
DDoS	Distributed Denial of Service
DNB	De Nederlandsche Bank
DSTV	Digital Satellite Television
ICT	Information Communication Technology
IEC	International Electro technical Commission
ISA	Information Security Awareness
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISM3	Information Security Management maturity model
ISMM	Information Security Maturity Models
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Information Security Policy
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NBE	National Bank of Ethiopia
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
RAID	Redundant Array of Inexpensive Disks
SPSS	Statistical Package for the Social Sciences
SSE-CMM	System Security Engineering Capability Maturity Model

CHAPTER ONE

INTRODUCTION

This section provides basic background for the research followed by motivation and problem statement. It also presents the research question, objective, scope and significance of the study. The chapter concludes by presenting organization of the study.

1.1 Background

Information communication technology (ICT) is playing vital role in the globalized economic sphere. It is widely adopted by various organizations like industrial enterprises, manufacturing companies, health sector, financial sector, educational system in their day-to-day operations. ICT has become a major driving force for economic growth and development, thus technological change and innovations could be a powerful process that opens up opportunities to increase social welfare and benefits for societies. The dynamics of events in the current competent financial world is also making financial organizations be dependent on this technology (Redlin et al., 2017).

The widespread use of ICT helps financial sectors to meet the customer need in various ways. In line with this, banks are widely adopting different technology solutions like core banking, mobile banking, internet banking, Cheque clearance, foreign remittance and so on. This made the banking sector highly dependent on ICT to conduct business and also indicates the priority required for safeguarding information resource, since information is an asset like land and labour (Ryan, 2006).

Even though these dynamically emerging technologies have positive impact on financial institutions, it has also risk if the organizations fail to protect their information assets from any cyber-attack (Malik et al., 2012). This is mainly because attackers are engaged in continuously developing malicious programs or electronic signals which alter, disrupt, degrade or destroy the whole or partial distributed system of networks (Waxman, 2013). As a result, one of the most difficult problems for financial institutions is information system security.

Information security management is described as the task of safeguarding information against any attack. which comes through networks of organizations. In order to ensure the business continuity and minimize the damage which will happen on the business and maximize the investment and

business opportunities, the information systems have to be secured and protected (Ladan et al., 2006). This in turn shows that an information systems security is a critical issue in an organization to make the organization ready to protect information assets from any security threats.

The use of information technology in developing countries is emerging and has got considerable attention in recent days. Number of researches are conducted in order to know the challenges and prospect of the actual adoption of information technology to get better result. Significant productivity has gained by developed countries but not developing countries, yet in this regard developing countries are investing on IT rapidly (Shih et al., 2014).

1.2 Motivation

Evaluating the information systems security capability helps to identify potential threats and existing vulnerabilities (Rainer et al., 1991). In recent days security threat is rapidly growing and the technological environment requires organizations to continuously adapt to changes and accommodate different kind of competing mechanisms. Saleh (2012) revealed that the importance of building information systems security to the organization and regular evaluation of information security maturity level helps to ensure the confidentiality, availability and integrity. This implies due attention to information systems security and the need to conduct study in this topic periodically.

The widespread use of information systems and related components allow organizations and individuals to connect with the global environment. These interaction and connectedness to the global sphere emerges with security threat beside its importance. Hove et al. (2013) iterated that information security attackers are not limited with geographical sphere and develop themselves for a better attack as the technology grows up. This indicates that financial institutions have to protect their information assets from any security incidents.

According to Luis et al (2006), before implementing information systems security measures in an enterprise, its mandatory to determine the maturity level of information security governance Information security management fails because there is no information security regulation Information and Related Technology Control Objectives (COBIT) IEC International Electrotechnical Commission ISM De Nederlandsche Bank ICT Information Communication Technology IEC. Following the step for information systems security, the existing information

systems security maturity level have to be defined and evaluated through different dimensions (Saleh M, 2011).

The cybercrime study annual report on 2017 stated that the annual cyber-attacks are rising every year with 27%, from average of 102 to 130 (LLC, 2017). Ransomware attacks are increasing by double and information security incidents like WannaCry and Petya affected thousands of targets and altered the function of public services, financial institutions and large companies across the world (Ponemon Institute Report, 2014). Based on reported figures, the high rate of increase in information systems security threats urges organizations to re-examine their information systems security maturity periodically.

The purpose of information systems security is ensuring the confidentiality, integrity and confidentiality of information assets that an organization owns. So, implementing appropriate control measures for protecting the information asset plays vital role towards minimizing the impact of security related threats and organizational vulnerabilities.

Banking sector is directly impacted by information security threat of different nature. Full or partial disclosure accelerates the diffusion of attacks, increases the penetration of attacks within the target population, and increases the risk of first attack after the vulnerability is reported (Ransbotham, 2015). Hence ensuring the confidentiality, integrity and availability have to be accompanied by the sector. A recent research by Ejerssa (2018) indicated that information security maturity is a key agenda for developing countries and is not sufficiently addressed. Ethiopian banking sector information security maturity is below the expected and their information security is insufficient (Beshah, 2017). Therefore, resolving the information security agenda requires high priority. Hence analysing the security maturity level will help financial institutions to take necessary action to protect their environment. The aim of this study is to do systematic investigation on the current information systems security maturity by analysing the current working environment and provide recommendation for improvement.

1.3 Statement of the Problem

Information security maturity level has hierarchy from lowest to highest, this can be achieved through applying different security maturity level measurement towards the security mechanisms. According to Saleh (2011), information security level can be affected by four different domains:

the organizational governance, the information security culture, the architecture of the system and service management. According to Negash et al., (2019), many security breaches are not caused by the faultiness of technology implemented rather users of the technology and the behaviour of human. Thus, there are many factors which contribute to failure in information security.

These day's financial sector is in high competition and thus implementing different technologies that can help to perform better. Since the financial sector is considered as a backbone to the economy, its information systems security has to be well designed, implemented and measured periodically. A more secured information sharing in an organization is considered as good approach in increasing the organizations effectiveness, efficiency, performance and decision-making capability (Binti & Julius, 2013). However, the behaviour of information sharing is very complex and grow dynamically, so it is mandatory to investigate and analyses the potential risks to ensure information systems security maturity regularly.

Information security measures are designed and implemented in an organization to demonstrate and elaborate the organization's approach to ensure information security. The information security mechanism consists of people, policies, infrastructure (Ejerssa, 2018) design to address the challenges of security breaches revolving around the secured and valuable asset of an organization. According to Ejerssa (2018), information security maturity level in higher educations in Ethiopia is found unsatisfactory. In fact, organizations are different on their structure, kind of information they have and the capacity to handle information securely. Hence, requirement for protecting information security mechanism is also different.

According to a study conducted by Toyigbé et al., (2015), conducting the measurement on information systems security using consistent metrics improves the ability to understand it and control it. Measuring the information systems maturity level leads to control and protect the threat that comes towards the organization and eventually helps to take improvement on information security handling mechanism. *"If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it."*[1].

(Bogale, 2018) on his part pointed out that most of the information security components are developed and implemented based on western perspective, without considering the actual need

[1] Quote by Lord Kelvin. "To measure is to know."

and working structure. Hence this issue misleads an organization to understand its basic requirement and prohibit from achieving highest objective of information security maturity level. To meet the information security objective, knowing the maturity level of the existing security mechanism plays vital role.

The fact that recent research conducted on information security of financial sectors in Ethiopia revealed that the information security protection and governance culture are unsatisfactory (Negash et al., 2019). Other local studies have been performed, such as an evaluation of the insider threat in the Ethiopian banking sector (Amare, 2015), cybercrime governance (Hailu, 2015), the policy towards implementing information security (Negussie, 2015), designing framework for information security implementation (Tebkew, 2016), designing framework for information security awareness creation (Kebede, 2019) , cyber hygiene practice for employees (Deferew, 2020), information security incident response management (Negash et al., 2019) and designing framework to manage human factor towards information systems security (Abebe, 2020). There are also other related works by (Beshah and Bayu, 2017; Ejerssa, 2018; Gera, 2019) those researchers try to address the information systems security maturity level on Ethiopian public universities and Hospitals in Addis Ababa. Even though those studies contribute an ultimate solution to address different information security problems, their intention was not on measuring the current information security maturity level. They mentioned that there is lack of study on the area of information security maturity level and recommend to conduct on the issue in regular basis. Hence, this study tries to fill this research gap and aims to identify the information security maturity level in the private banks in Ethiopia and propose possible solutions to fill the gaps. This will help the banks to know their security maturity level and take corrective actions so that they can withstand potential cyber-attacks.

Most of the researchers are agreed on dynamisms of information systems security threat. Thus, to protect the information from those security threats organizations have to clearly know their requirement of information systems security maturity level assessment tool. The major problem with information systems security is not due to lack of the knowledge to protect information, but the way how to apply information security management based on the standard and the measurement metric to evaluate the maturity level of information systems security. Information Security proliferates into various domains of knowledge and becomes more context aware (Slusky

& Partow-Navid, 2012). Hence from this we understand that information systems security management is different in nature from one country to another also different from organization to organization. For instance, the financial institution found in Netherland can measure their information security maturity level based on the DNB information security maturity model assessment tool. However, there are no requirements on control objective level of what is necessary for financial institutions to reach a certain maturity level per controls (Pijpers, 2015). Financial institutions in Netherland are expected to achieve maturity level of 4. This shows the model is designed to the country specific information systems security maturity model measurement.

1.4 Research Question

Based on the research gap presented in the problem statement in section 1.3, this research tries to answer the following research questions.

I. Where is the information systems security maturity level of Ethiopian private banking industry?
II. How can the security gaps be improved to enhance the information security maturity of the private banks?

1.5 Research Objective

1.5.1 General Objective

The ultimate goal of this research is to identify information systems security maturity level and figure out security gaps for Ethiopian private banking industry.

1.5.2 Specific Objective

- Review related literature to identify maturity models for information security maturity measurement.
- To identify an assessment tool to measure information security maturity level.
- Identify problems and efficient approaches in managing Ethiopian private banks' information security maturity level in regard to the chosen international guideline.
- To indicate potential improvements which can be taken to have better information systems security maturity level in the sector.

- To recommend possible solutions to improve information systems security maturity of the banks.

1.6 Scope of the Study

Due to time, cost and the sensitiveness of measuring the information systems security maturity, it does not cover all banks in the country. The scope of this study is thus limited to address the maturity of information systems security of private banks in Addis Ababa, Ethiopia. Sample of four banks selected (Bank 1, Bank 2, Bank 3, Bank 4) for the study.

1.7 Significance of the study

The outcome of this study helps the banking industry to visualize their current information protection capacity and identify security gaps that need to be addressed. Maturity of information systems security indicates the degree of development and strength of an organization's security measures to mitigate risks threatening its assets. The study outcome also helps the top management in the banks to check necessary security measures when they sign deal with software vendors. It also helps to give awareness and insight for IT staffs and Information security management department to properly manage and monitor the information systems security. Other banks and related financial institutions can also benefit from the research output by evaluating their information systems security level with the assessment tool and technique used in the study. Finally, the output from this study can be used as an input and reference for future researchers.

1.8 Organization of the study

This thesis is organized in to five chapters. chapter one discusses the overview of information systems security, the statement of the problem, the research questions, the research objectives, the scope of the research, and the value that the study would provide contribute to the organization are discussed in significance of the study sub tittle. Chapter two discus the literature review in information systems security and related disciplines. In this chapter main and basic conceptual and empirical literature is reviewed and presented. Chapter three provides the detail description about the research design and methodology used. Under this the data collection, the population, sampling techniques and sample space are presented. Chapter four deals with the data presentation, analysis and discussion. The final chapter, chapter five is the final portion for this study and based on the

research output this section gives recommendation to have good information systems security maturity level, the conclusion, limitations of the study and future research areas also presented in this chapter.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The aim of this chapter is to go over all that has happened so far, the conceptual and related literature to provide an understanding of information security maturity level. The literature review aims to identify the concept of information systems security maturity in an organization based on different researches conducted locally and abroad. The review is conducted based on a detailed reading of selected body of references related to information systems security. This chapter covers the following major topics: an introduction to information security, information security operations, information security issues, resources and best practices, information systems security management standards, and information security continuity, Information security maturity, models of information security maturity, evaluation of information security maturity, factors affecting information security maturity, information security in financial sectors, and a summary of related works.

2.2 Information Security

Information is a valuable asset that can be transmitted through electronic media or physical form. Information is defined as an asset valuable for a given institution, and is presented different formats like printed, written, electronic, audio, video and oral (ISO/IEC27002:2013). In recent days with the development of information technology, people are highly dependent on digital technologies. Information has become a key asset these days. According to Patil (2019), 21st Century is called the “Information World”. Hence the world comes to get difficult for those who have not updated themselves with recent knowledge about the digital technology.

As information is a vital asset, security concern associated to it. Security is a means of protecting something from damage. Many researchers and practitioners have tried to define security in various ways. Patil (2019) defines security based on a computer system security perspective as information security is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or

physical location to another. Information is taken as an asset and has data with a set of values for a given organization or person, which is a resource of extreme value in today's society. The information has value when it is stored and accessed by authorized users in a protected way.

Information asset may be affected by the misuse behaviour of users, by the surrounding environment and system structure, by malicious software for the purpose of stealing and theft, destroying or altering the information content. The rapid development of information and communication technology allows people to store and transmit information at any time and at any place. Thus, unauthorized access to the information content is an issue mainly during storage and transmission of information. Hence information security is essential for some organizations and critical for others. Information security refers to a process of techniques and methodologies designed and implemented to protect information from unauthorized access, use, misuse, destruction, disclosure, modification, or disruption (Malik, 2011). It is a set of practices applied to keep information secure from unauthorized access or alterations.

In general, information security is concerned with protecting the confidentiality, integrity, and availability (CIA) of corporate data, systems, and information communications technology. (Pillitteri et al., 2017). Likewise, the ISO/IEC 27002 international information security model establishes information security as the protection of data's confidentiality, integrity, and availability, shortened as CIA. However, ensuring those features is more than just a problem of IT security; it also includes policy and procedure, governance, and workflow management concerns. (Tredinnick, 2016). The nature of the digital infrastructure and the daily working activity of society makes it easier to manipulate information at high volume. Hence millions of documents can be carried out on the smallest device and transmitted globally with a high-speed data connection.

The CIA is considered as a basic standard for protecting information and is widely implemented information security model that can promote an organization's effort to employ policy and procedure aimed at keeping the data secure (Perrin, 2008). It is a security model created to guide information security policy and procedure within an organization. Unlike other information security standards, the CIA triad doesn't have a single creator rather it emerged over time. Keeping the CIA triad in mind when an organization implements an information security policy helps the security team to make a productive decision about the confidentiality, integrity, and availability of a set of data.

Figure 2.1: CIA Triad structure (Frunhlinger, 2020)

The detail explanation on the CIA triangle is presented based on Frunhlinger (2020) as follows:

- **Confidentiality: -** is the security principle which controls access to the information. It ensures the access has granted only for authorized users and not allowed for unauthorized requesters. Organizational data can be categorized according to data type and content. Hence the access can be granted based on the sensitiveness of information. Confidentiality needs the enforcement of appropriate data access level. In doing this it often involves separating information into a discrete collection organized by who should have access to it and how sensitive it is. An example of the most common methods to protect confidentiality is data encryption, access control list, file permission level, biometric verification, security tokens, and digital certificates.
- **Integrity:** - Data integrity is about protecting the data from modification and deletion by unauthorized parties. The consistency of data should not be altered while it is stored or in transfer from one destination to another. Version control can be used to prevent intentional /unintentional changes and deletion from authorized users. The other controlling measures to ensure the integrity of data is detecting the data change that might occur due to server error and some changes on the information systems infrastructure. In case of any data integrity failure, the data backup and redundancy plan help an organization to restore the affected data into its original state.
- **Availability:** - is to guarantee reliable and constant access to data for authorized users only. To ensure the availability of data and to resolve the bottleneck and communication

throughput which comes through time. Some of the precautions taken to ensure the availability of data is redundancy, failover, RAID (Redundant Array of Inexpensive Disks), and clustering. In case of any data loss, ensuring the availability will comply ensuring the data recovery and business continuity.

2.3 Information Security Roles

The use of information technology has dynamically grown with the latest business opportunities (Deferew, 2020). However, these opportunities have created a risk concerning information security. In recent days especially in the last two decades, personal and professional lives are interconnected with technology. People can conduct high transactions from their mobile, they can operate their bank account, buy, sell, and order what they want from their simple device using the digital technology. While this convenience made people's lives easier, it also made easier for cybercriminals to gain access to sensitive information wherever it lives or wherever it is traveling across the communication medium (Hove, 2013). Information systems hackers are eventually finding a way to get data which they do not have legal access to it. The information security professionals are also on the front line for the data theft battle to protect against the continually evolving threats.

Information has a huge impact on the competitiveness between firms and, it is the most valuable asset for organizations in which it is considered as a critical resource, which promotes and enables an organization to achieve business goals. Hence information is considered a lifeblood for most organizations. Information systems security plays a vital role in protecting the information from accidental loss, deliberate dissemination, modification, and damage. The controlling mechanism to ensure the information security includes logical, technical, and administrative management of information security. These mechanisms should properly be integrated to address the security-related issues. Information security is not only taking into account on the design and development phase of information security management, it also considers the infrastructure domain which requires technical solutions (ISO/IEC 27001, 2016).

Information security has evolved from its traditional orientation, which is mainly focused on technology to become part of the firm strategic alignment, enhancing the alignment between business goal and information security policy (Olijnyk, 2015). Hence information security is

considered a business enabler by creating value for organizations, such as competitive advantage. Furthermore, information security plays a vital role in companies' daily operation, since the integrity and confidentiality of information must be secured and available when it is required by authorized users (ISACA, 2012).

Ensuring the confidentiality, integrity, and availability of the information is not a one-time operation, it requires regular security monitoring, information security data log analysis, detect security incidents, mount incident response and utilize the latest technologies and possess to enhance security capability and the firm will have confidence in the business goal achievement (Catarino et al., 2016). Another functionality of information security is that it also provides security mitigation techniques, encryption to secure information, design security system for major components of security systems, install and manage organization-wide security system.

In general, to provide convincing arguments for information security management, Information Security Officers have to identify risks to organizational infrastructure and develop information security maturity measurement system capable of determining the effectiveness of controls introduced in accordance with the relevant business-standard. In line with this, senior management plays a vital role to ensure the availability of resources related to security management, the information security team is also responsible for verifying the functionality of the implemented security tools based on the policy and procedure regularly.

2.4 Information Security Threats

An information asset of an organization must be protected from information security threats. A threat to information asset is defined as any situation or occurrence that has the potential to damage an information system by deleting, destroying, modifying, or disclosing data, or by denying service (Bowen et al., 2006). The vulnerability to information security is a serious one that act to corrupt or steal data of an organization's system or the entire organization. And an event that results in a data or network breach is called a security incident (Bowen et al., 2006). Such system breaches or harms happen when the threats exploit vulnerabilities in the information system.

Malicious software or malware which are developed to alter the main functionality of information systems security increased by 25% in 2018 (Thebestvpn, 2019). These malwares are used by attackers to compromise the confidentiality, integrity of data, and availability of the system. The most common types of malwares are worms, viruses, Trojan horse, spyware, ransomware, WannaCry, adware, and scare-ware. DDoS (Distributed Denial of Service) is also a kind of attack and its main effect is on the availability of data.

Due to high dependency on information systems, organizations are facing information security risks which can cause the organization to lose its business and reputation (Moller, 2017). This issue takes the organization's attention to information security management practices. Therefore, to have an efficient information security protection capacity, organization consequently implement different technical and administrative measures to mitigate threats which comes towards the information management system. According to Barki (2010) employees working in an organization are the weakest link for security breaches. This also implies that the awareness and behaviour of the user's also have an influence on the maturity level of information security advancement.

The global information sphere is rapidly developing. Modern information technologies represent not only new opportunities in solving various problems, but also create fundamentally new challenges and threats (Tershukov, 2019). The emergence of information technology and the development towards the expansion of the networking system has come with advantage for firms to facilitate their business. On the other hand, the information security threat and vulnerabilities of the system is a challenging issue that an organization has faced (Tershukov, 2019). The security threat damage can range from small losses to the entire information systems destruction.

The life of modern society is inconceivable without modern information technologies (González et al., 2019). Computers serve banking systems, control the operation of nuclear reactors, distribute electrical energy, monitor train, and aircraft schedule, manage traffic controlling system, control spacecraft, etc. Computer networks and telecommunications can determine the reliability and strength of the country's protection and security systems. Computers provide storage of a huge amount of information. And its processing output and facility will be provided to consumers. There are several types of security threats to information like hacking, viruses, worms, denial-of-service, eavesdropping, packet alteration, and so on (Tershukov, 2019). Thus, the threat to information

security is one of the most important problems of modern human life and an organization need to know where it comes from and how to protect itself from damage.

Different researchers revealed that information systems security threats can originate from inside or outside of information systems facility and can be intentional or unintentional. Information security threats can also be classified as natural and artificial threats. Threats are increasingly complex and can take any opportunities for vulnerability within applications and network infrastructure. Any product whether hardware or software is exposed to a security threat and can cause extensive damage to the organization. According to the Computer Security Institute survey report from mid to large-sized companies' total losses from security damage for 2006 amount is about $141,496,560 (Gordon et al., 2004). This shows information security threats can result in significant financial losses and damage to the information systems resource.

Extant literature reveals that there exists different classification of Information security threats. NIST classifies information systems security threats as follows:

- Errors and Omissions – these are significant information security threats that are usually underestimated. But as defined above security threats are every event and occurrence that can lead to information systems (hardware, software data ware, and network) integrity breaches and mitigation. Therefore, errors and omissions are basic information security threats. Employees can make mistake during the data entry, later it used as a data source. The fact that it's not possible to build-in application mechanisms for every possible type of data entry error control. These kinds of errors did not happen only on data entry. It can also happen during the programming and information systems development process. This results in serious consequences on information systems security.
- Fraud and theft – this type of threat is basically misusing of a victim's information and existing financial accounts. Fraud is a property crime where the hacker tries to achieve an unfair advantage over the information handled by others. Computer frauds and theft can be performed either by insiders or outsiders. Since the employees working in an organization has unlimited access to the information systems and resources, most fraud and theft are originated from insiders. According to Lawrence et al (2006) "insiders constitute the greatest threat to computer systems". American safe ware insurance analysis showed $882 million USD has a worth of personal computer theft in 2002.

- Loss of Physical and Infrastructure – this can be realized in many different ways, for example loss of electric power, loss of communication between parties, earthquake, flood, fire, lightning strikes, etc. This kind of information security threats cannot be under full control and protection capacity of information security professionals.
- Hackers – this kind of information security threat has not limited by boundary and the attack can originate from everywhere. The term hacker refers to a person who tries to gain unauthorized access to information systems and resources. Most of the time the source of this threat emerges from outsiders and their main goal is basically not defined. It could be data theft, deletion, change of data, etc.
- Malware – it is a type of information security threat that incorporate computer viruses, Trojan horses, Worms, logical bombs, and other forms of undesirable software. Hence computer viruses are programs which individually replicated and attached with executable files. When the user starts to execute the .exe file automatically the virus attached itself to the computer systems and replicates into the network system. Trojan horse is a type of malware that masked as legitimate software. This software can be hired by cyber-thieves and hackers trying to gain access to users' machines. Users are typically cheated by some form of social engineering into loading and performing Trojans on their machine.

Accordingly, the constant expansion and deployment of new viruses and worms, the abundance of internet attacks expose information to the security threat. The information security threat can be classified based on their security threat frequency, intensive area coverage, and the source of security threat (Huntinski, 2007). One of the basic prerequisites for a fruitful information systems security management process is the usage of certain security threat classification.

2.5 Information Security Management

Information security management is the framework for ensuring the effectiveness of information security controls over information resources to ensure no repudiation, authenticity, confidentiality, integrity and availability of the information (Hentea, 2008). Organizations need a systematic approach for information security management that addresses security consistently at every level. However, the security infrastructure of most organizations came about through necessity rather than planning, a reactive-based approach as opposed to a proactive approach like Intrusion detection systems, firewalls, anti-virus, virtual private networks, encryption and biometrics are

information security management technologies in use recently (Gordon et al., 2004). Information security management helps an organization to manage the security of information and assets. It determines the process of protecting information assets to preserving confidentiality, integrity and availability of information (ISO/IEC27001:2013). It helps an organization in managing and mitigation the various threats and vulnerabilities to an asset and helps to balance management effort in all organizational aspects (Al-Dhahri et al., 2017). Moreover, information security management encompasses the set of policies and procedural controls that IT and business together implement to secure their informational assets against threat and vulnerability.

The increase in an enterprise data and the information security threat led to significant development in the field of information security management. The information management system is a type of management system that deals with information security (ISMS) and it involve four essential components which are security process, personnel, management principle and resource (BSI–Standard 100, 2008).

Figure 2.2: Components of an information security management system (ISMS)

Source: BSI – Standard 100 (2008 p.14).

All processes relating to monitoring and supervision for the purpose of achieving the institution's goals are included in information security management. The information security management system is the component of information management that deals with information security (ISMS).

The ISMS defines the tools and methods that the organization may use to plan, conduct, and monitor operations, as well as improve and control tasks and activities aimed at achieving information security.

2.6 Information systems Security Management Standards

Information security is critical to the organization's activities because it protects its assets from both internal and external attacks. And, to ensure that the organization's information security deployments are sufficient, there must be a strategy or guideline that establishes information security governance. Establishing an effective set of information security management is a time-consuming and resource-intensive process that necessitates unique resource utilization and knowledge. (Rainer et al., 1991). As a result, information systems security management standards that provide instructions to the business by establishing and implementing a set of controls conducive to an acceptable level of information resource protection are necessary.

Information security is a business enabler that is inextricably linked to stakeholder trust, either through managing business risk or by producing value for organizations, such as strategic advantage. (ISACA, 2012). Moreover, information security standard plays a key role in a company’s daily operations, since the integrity, confidentiality, and availability of their information must be ensured and accessible for granted users. Especially those organizations that deal with sensitive information should be ready for the threats, because the information is the most valuable asset, and having the right information at the right time can lead to more profitability than loss (deSouza, 2010).

According to (Rhodes-Ousley, 2013) Policies, protocols, processes, and guidelines are the primary components of an information security standard. Together, these elements constitute the full concept of a maturity program. The capability maturity model (CMM), which assesses the robustness and repeatability of a business process, is often used in information security.

- **Policy** is a high-level declaration of requirements. A security policy is the primary means by which management's security requirements are communicated to the programmers, installers, maintainers, and clients of an organization's information systems team. A security strategy serves as the basis for a robust and successful security program. A successful security policy is a high-level, brief, formalized statement of the security

practices that management wants workers and other stakeholders to adhere to. A security policy should be straightforward and simple to implement so that everybody can adhere to the guidelines outlined in it.

- **Standards** clearly state how to setup computers, install and update applications, and use computer systems and other valuable functions to comply with the policy's objectives. Standards are the current policy extended version into the reality; they define technology options, operating systems and behaviours. Security managers in charge of IT infrastructure will typically spend more time writing standards than they will on policies. Policy statements are plain, straightforward, and somewhat general in nature. The policy is interpreted by standards to the degree of specificity required by a technical expert.
- **Procedures** specify stage process instructions for completing various tasks associated with policies and standards the process is a series of steps that a system administrator will follow when installing and configuring server environments.
- **Guidelines** are providing recommendations on how to accomplish the security policy's aims, but they are just guidelines, not laws. They are an effective communication tool for informing people about policies and instructions. They follow best practices when it comes to using technology systems or behaving in accordance with management's expectations.

It is imperative for organizations to use an information security management system (ISMS) to effectively and efficiently manage their information assets. ISMS help an organization to set policies, standards, procedures, and guidelines to define, construct, develop, and maintain security. Since information security has a very important role in supporting the activities of the organization, information security management standard and benchmark is required which regulated governance over information security. There are widely used information security standards, which leads to information security such as ISO27001 (International Standard Organization), BS 7799 (British Standard), PCI-DSS (Payment Card Industry Data Security Standard), ITIL (Information Technology Infrastructure Library) and COBIT (Control Objectives for Information and Related Technology) (Tuan et al., 2011).

2.6.1 ISO/IEC 27001

ISO/IEC 27001 provides a model and detailed guidance for reducing an organization’s exposure to an information security risk, as implemented through an information security management

system (ISMS), using this standard enables organizations of any kind to manage the protection of assets including financial data, proprietary information, employee records, and information entrusted to third parties. The requirement was released by the International Organization for Standardization (ISO) on 15 October 2005 (ISO/IEC27001, 2005). Basically, ISO/IEC 27001 defines an Information Security Management System (ISMS) and supplements the ISO/IEC 17799 'code of practice' standard, which was first published as BS 7799-1. The two principles are closely related and aligned, yet they serve unique functions.

The ISO/IEC 270001 Information security management adopts the well-known PDCA (Plan-Do-Check-Act) process approach as illustrated in figure 2.3 (ISO/IEC27001, 2005). PDCA helps the management to continuously manage the information security improvement, Since ISMS necessitates frequent monitoring and analysis to determine if risk management controls are still efficient.

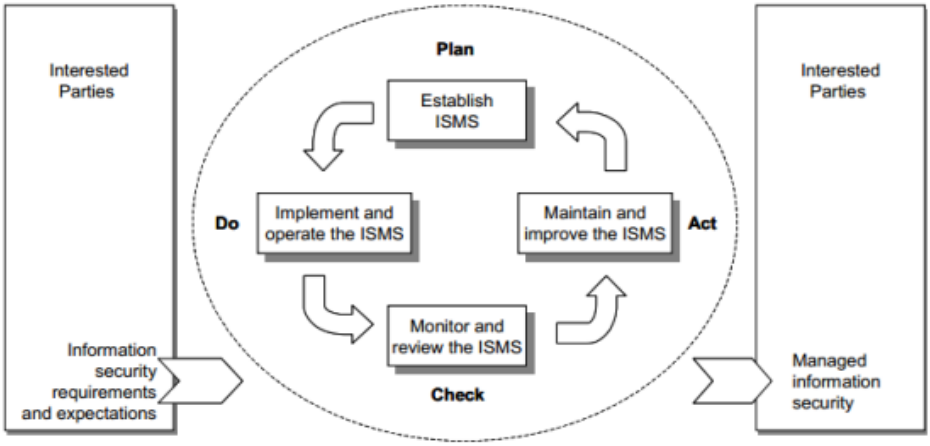

Figure 2.3: Application of the PDCA model to ISMS structures

Source: ISO/IEC 27001 a standard for information security management (2005, p.6).

The international standard of ISO 27001 specifies the specifications for creating, implementing, running, tracking, updating, maintaining, and enhancing a documented ISMS within the organization (Tuan et al., 2011). ISO 27001 has two parts: -

1. ISO 27001:2005, Information technology - Security techniques – Requirements for Information Security Management Systems Which offers a management approach to the

development of a fit-for-purpose information security management system, as measured by the information security needs and expectations of all stakeholders.

2. ISO 17799:2005, Information technology - Security techniques – Code of practice for ISM. organized into 11 areas and 39 security control goals, each of which is focused on a specific field of information security concern confronting an organization.

For the investigation of Information security management of Ethiopian private banks which undertakes a descriptive research using ISO27001:2013 which is organized into 11 areas and 39 security control goals, each of which is focused on a specific field of information security concern confronting an organization. This internationally recognized standard is used to assess the degree of information security maturity. Depending on the ISO 27001:2013 standard's main focus areas, as shown in table 2.1. As a result, the study employs the Information security (Annex A.5 – A.18) criteria to assess information security maturity and using the SSE-CMM maturity model the study categorizes sampled banks information security maturity level.

Table 2.1. Domains, objectives and number of controls in Annex of ISO 27001:2013 ISO/IEC 27002

Source: Candiwan et al., (2016, p.3).

No. Annex	Domain of ISO 27001:2013	No of Objectives	No of Controls
A.5	Information Security Policies	1	2
A.6	Organization of information security	2	7
A.7	Human resource security	3	6
A.8	Asset management	3	10
A.9	Access control	4	14
A.10	Cryptography	1	2
A.11	Physical and environmental security	1	15
A.12	Operational security	7	14
A.13	Communication security	2	7
A.14	System acquisition, development and maintenance	3	13
A.15	Supplier relationships	2	5

A.16	Information security incident management	1	7
A.17	Information security aspects of business continuity management	2	4
A.18	Compliance	2	8
Total		34	114

The International Organization for Standardization (ISO) defined ISO 27001 in 2005, and it was modified in 2013. ISO specified the basic principle, execution, repair, and management of one of the information security organizations. (Somepalli et al., 2020).

ISO 27001 specifies effective strategies for information security management, risk assessment, and implementing security measures within the framework of an Information Security Management System (ISMS), while ISO 27002 specifies controls and good practices that can be used as guidelines when choosing and implementing measures to achieve information security. (Diamantopoulou et al., 2020). both focus on the minimization of risk realized by data breaches. ISO 27001 focuses on reducing risks to information security by compelling organizations to produce ISMS that are continuously maintained and improved.

The ISO/IEC27002:2013 international standard's method approach to information security management encouraged businesses by emphasizing the following points.

- Understanding the information security requirements of the organization, as well as the need to define information security policies and goals.
- Putting in place and maintaining policies to deal with an organization's information security risks in terms of the organization's overall business risks.
- Regularly monitoring the efficiency and effectiveness of the ISMS
- Progress that is consistent and based on quantitative metrics.

The ISO/IEC 27001 and 27002 guidelines are based on BS 7799: In 1995, the British Standard Institution (BSI) issued the BS 7799-1 guideline, titled "Information security part I: Code of practice for security management." In 1998, a second portion, BS 7799-2, titled "Information Security Part II: Information Security Management System (ISMS) Standard," was produced. The British Standard BS 7799-2 is a collection of requirements for development (Barlette & V. Fomin,

2009). The ISO (International Organization for Standardization) has adopted both of the BS standards mentioned above as international Information security management directives:

- In 2000, BS 7799-1 was republished as ISO 17799, and in 2007, it was renamed ISO/IEC 27002.
- In 2005, BS 7799-2 became ISO/IEC 27001 standard.

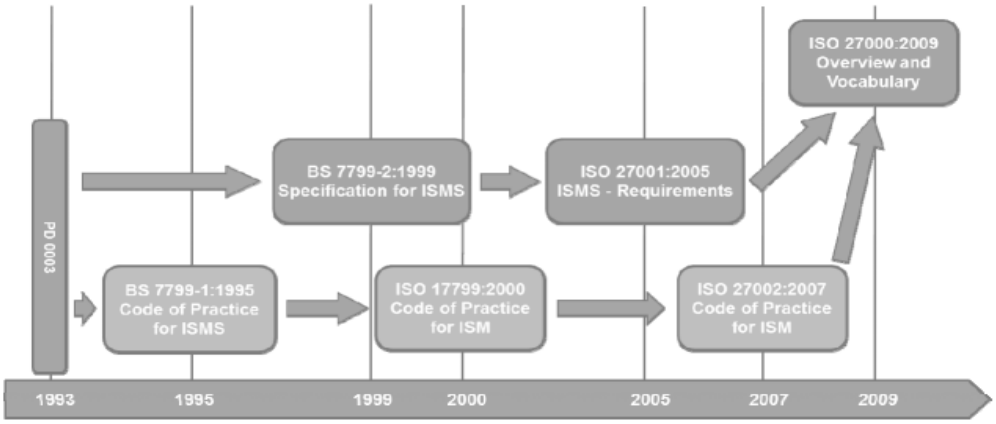

Figure 2.4. ISO 27000, ISO 27001, and ISO 27002 standards architecture growth

Source: Georg (2013, p.95).

The coding criteria in ISO 27001 are extended and clarified further in ISO 27002 as a guideline. The ISO 27002 standard lists and specifically describes 39 control objectives and 134 security monitoring steps. The control objectives are described below, divided into 11 domains. The ISO 27002 standard goes into greater detail about these (Georg, 2013).

1. **Security policy:** Provide management, guidance, and support for information security in accordance with organization practices and relevant laws and regulations.
2. **Organization of information security:** To ensure the protection of the institution's information and information processing facilities that are viewed, stored, interacted with, or handled by third parties.
3. **Asset management:** To achieve and sustain adequate security of organizational properties, as well as to ensure that information is adequately safeguarded.

4. **Human resources security:** To reduce the risk of loss, theft, or misuse of resources by ensuring that staff, vendors, and third-party users recognize their obligations and are qualified for the positions they are being considered for.
5. **Physical and environmental security:** To prevent unauthorized external entry, destruction, and disruption with the properties and information of the company.
6. **Communications and operations management:** In accordance with third-party service delivery arrangements, enforce and sustain an acceptable level of information security and service provision.
7. **Access control:** Controlling information access by preventing unauthorized access to the network services, software platforms, and data stored in information system.
8. **Information systems acquisition, development and maintenance:** To ensure that protection is an essential component of information systems, as well as to avoid errors, loss, unauthorized alteration, or misuse of data in systems.
9. **Information security incident management:** To protect the information security events and vulnerabilities in information systems are recorded in a reasonable timeframe, allowing for appropriate remedial steps.
10. **Business continuity management:** To mitigate business interruptions and defend vital business processes from the impact of major information system disruptions or disasters, and to ensure their effective continuation.
11. **Compliance:** To guarantee that projects respond to corporate security policies and standards, as well as to increase the performance and minimize conflict with the information security evaluation process.

2.6.2 ITIL

ITIL is a framework for information technology designed to standardize the planning, delivery, maintenance and monitoring of the overall life cycle of IT (Information Technology) services and process within an enterprise (IBM Cloud Education, 2019). Its goal is to improve efficiency and achieve predictable service delivery. One of the most important aspects of ITIL is its maturity. The configuration management database (CMDB) serves as the central authority for all required components to provide an IT facility, such as systems, applications, devices, IT implementations, databases, and clients. (Hernandez, 2019).

ITIL is designed based on the IT service requirement which adds guidelines on service strategy design, transition, and operation. It also provides a way for businesses to continuously improve services. It has five key stages that help the framework to align business with service management (Hernandez, 2019).

- **Service Strategy**: - It is concerned with the company goal and consumer requirements, as well as how to match the business and service goals.
- **Service Design**: - It is a practice overview for IT procedures, design, and documentation of the service monitoring system.
- **Service Transitions**: - Recommendation on change management and release activities also assists the administrator in managing environmental interruptions and change.
- **Service Operation**: - Provides guidelines and measures for managing IT services on a regular, weekly, and yearly basis.
- **Continual Service Improvement**: - Provides guidelines on how to implement enhancements and regulatory changes within the ITIL process system.

2.6.3 COBIT

Information Technology (IT) has an important role for every company which uses information technology in its business activities and categorized as one of the factors in achieving company goals. IT will be optimal if only IT management is maximized. Proper management of IT in a company will certainly identify all forms of risk from the application of IT and the handling of the risks which will be faced. Hence, the company required an application that is needed to be implementing IT governance. The IT governance intended to provide building the policies and management of IT infrastructure, using the IT service by end-users efficiently, effectively, and safely as well as effective IT project management process (Matin, 2018).

COBIT is a means of measuring the standard of control Information technology is generally useful to balance risks and investment in the scope of information technology (Christianto et al., 2020). COBIT provides effective practice and efficiency to the entire framework and activity components in a flexible structure. This framework plays a vital role in the contribution of the fulfilment of business strategy needs, identifies the main IT sources and management control objectives. Company performance is a measure of the success rate of management in managing a company's resources, especially on investment management as an effort to create value for shareholders.

COBIT, in general, enables IT to be controlled and managed holistically through the enterprise, taking into account the full spectrum of end-to-end enterprise and IT operational duties and responsibilities, as well as the IT-related priorities of internal and external stakeholders. COBIT 5 is applicable to businesses of all types, whether for profit, not-for-profit, or government. (ISACA, 2012). According to the ISACA business framework for IT governance and management COBIT has 5 principles.

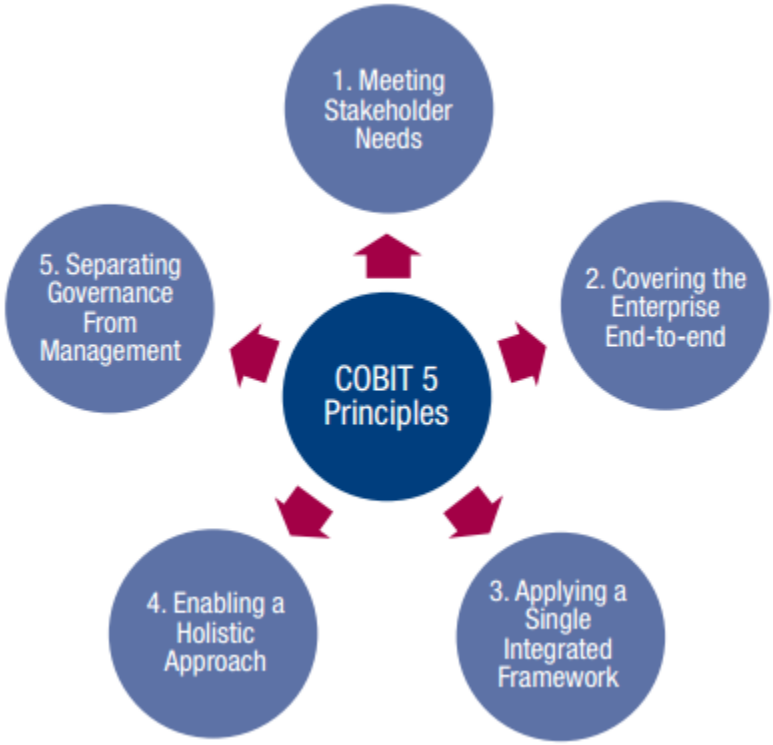

Figure 2.5. COBIT 5 Principles Source ISACA Personal copy or Rose C. (2012, p.13)

Meeting Stakeholder Needs: Enterprises operate to generate value for their stakeholders by striking a balance between profit realization and risk and resource optimization.

Covering the Enterprise End-to-end: COBIT 5 incorporates enterprise IT governance into overall enterprise governance.

Applying a Single, Integrated Framework: There are several IT-related guidelines and best practices, each of which provides guidance on a specific subset of IT activities. COBIT 5 is highly aligned with other related standards and frameworks.

Enabling a Holistic Approach: Effective and convenient corporation IT governance and management necessitate a holistic approach that takes many interacting components into account.

Separating Governance from Management: The COBIT 5 framework distinguishes between governance and management.

2.7 Information Security Maturity

Valuable information is more sensible to be vulnerable to information security threats (Eshlaghy et al., 2010). Moreover, the observance of the information security principle is taken as critical infrastructure in today's knowledge-based organizations. Hence, for an organization to achieve its goal and mission, regular monitoring and evaluation are required on the information security maturity level. Therefore, measuring the maturity level of information systems security of an organization would be vital in preparedness towards information security. One of the main advantages of monitoring information security maturity is to assess the security level and to protect information infrastructure from the increasing risks associated with technology evolution. Due to the continuous improvements in technology, information security threats continue to increase on a larger scale and are advancing at a faster rate than what the current frameworks can accommodate (Somepalli et al., 2020).

Information security maturity is a collection of characteristics or measures for information protection that reflect an organization's security program's capability and evolution. (Malik, 2012). In recent days each organization are exposed to threats and risks on their information systems due to the rapid evolution of cyber-attack. Moreover, the main risk is the organizations are failed to assess how can the protection level be raised to protect against the growing risks associated with technological advancement. However, there are a number of variables that may assist in assessing the extent of information security maturity. such as technology, people, and infrastructure (Al-Matari et al., 2020). The overall information security maturity includes information security and risk mitigation collaboration, an organizational strategy, and information security budget allocation. For an organization, their information security maturity level can be presented in different terminologies based on the measurement tool and techniques. According to Al-Matari and his colleagues (2020) The majority of frameworks and models describe information security maturity levels as non-existent (level 0), ad hoc (level 1), repeatable (level 2), specified (level 3), controlled (level 4), and optimized (level 5). The degree of information security maturity is determined by a number of factors. Physical and network infrastructure, the capacity to execute

regular operations, data storage and transmission management, and quality management are examples of these factors (policies, standards, and guidance).

2.8 Information Security Maturity Models

Maturity models have been extensively being used as a means of organizational development or measurement in the area of information technology. Any framework for performance analysis and improving efficiency can be considered as the basis, and if it incorporates methods for quality assurance, it is referred to as a maturity model. (Saleh, 2011).

Maturity refers to and describes the level of information security maturity, assessment, and safety. Information security maturity models are a systematic framework for meeting and fulfilling customer needs and demands by including the entire enterprise in the preparation and execution of breakthrough and quality improvement programs. It fits with the organization's business strategy and can have a positive impact on customer satisfaction and increase market share. To identify the strengths and weaknesses of an organization's information security maturity level, a variety of frameworks or models may be used to assess and identify the discrepancy between the security criteria standard and the actual working environment layout.

The aim of implementing an information security maturity model (ISMM) is to close the gap between business requirements with respect to the information security and to define the actual level of information security on preventing security threats (Spruit & Roeling, 2014). An organization business and information systems can be influenced by technical and non-technical aspects of information security services. Hardware, software, and network infrastructure are technological information security aspects, while ethical and cultural standards, legal and contractual documentation, administrative and managerial procedures, organizational and procedural protocols, and awareness programs are non-technical information security aspects. (Karokola et al., 2011). Therefore, the ISMM metrics must be designed with a focus to organization based and towards managing technical and non-technical security aspects.

Information Security Maturity Model is a technique that has been proved to be valuable in measuring different aspects of the security process of an organization (Borbinha, 2016). It constitutes a step toward a more coordinated and structured way of doing business in enterprises. The maturity model is made up of many "maturity stages," which are typically classified into five

levels, from bottom to top: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. The number of levels, furthermore, may vary depending on the type and the issues guiding the prototype. The progression of information security maturity from an initial state to a final desirable state is linked to the demonstration of a specific capability or the achievement of a specific target.

According to Ngwum (2016), ISMM is explained as a tool for assessing an organization's information systems capable of meeting security requirements, while ensuring the organization's objectives are met in the midst of security attacks and incidents. A variety of models must be developed in order to determine and investigate the strengths and weaknesses of a company's information security protection maturity. The goal is to identify a gap for both theory and practices that can then be connected using a process-oriented technique. The greater the company's exposure duration, the more vulnerable it is to threats and attacks. The severity of threats is minimized when companies are informed of their compliance requirements. (Saleh et al., 2012).

Studies on the Information Security Maturity Model the organization's information security automation dimensions (Osamah et al., 2020). It also strengthens organizations' protection by implementing vulnerability defensive measures. It identifies a collection of documents that are needed to carry out the appropriate controls. Then, it defines the automatic controls that have been implemented via a series of procedures. Eventually, it determines the appropriate security maturity level based on the organization's operations. As a result, the security maturity level is appropriate for the hardware and software environment in which it operates. The most common information security maturity models are taken from different pieces of literature and summarized below:

2.8.1 NIST

The National Institute of Standards and Technology (NIST) has released a framework that will help companies in critical infrastructures to minimize the risk of information security risks. It implements five security measures for institutions. These controls include data and asset identification, detection, security, response, and recovery (Osamah et al., 2020).

The National Institute of Standards and Technology (NIST) was founded in 1901 with the goal of promoting innovation in the United States and market conditions that promotes scientific measurement, standards, and technology to improve social security. (Sri et al., 2020). The NIST framework establishes rules for the activity of US enterprises. It will assess and develop the

capability of investigating, preventing, and responding to cyber-attacks. NIST version 1.0 was released in 2014, and version 1.1 was released in 2017. The National Institute of Standards and Technology (NIST) provided categorization, strategic plan, client, employees, interaction, meter, technical and instructional management, and success rates.

The list of security controls in Special Publication 800-53 can be widely used to secure information and information systems from conventional and modern persistent threats in varying functional, environmental, and technological circumstances. The measures can also be used to illustrate compliance with a wide range of governmental, organizational, and institutional security standards (Blank et al., 2020). Institutions are responsible for selecting the necessary security controls, correctly implementing the controls, and demonstrating the efficacy of the controls in meeting defined security requirements.

NIST guidelines adopt a multi-tiered approach to risk management through control compliance. SP 800-53 works alongside SP 800-37, which was developed to provide federal agencies and contractors with guidance on implementing risk management programs. SP 800-53 focuses on the controls which can be used along with the risk management framework outlined in 800-37 (Blank et al, 2020). The security controls are broken into 3 classes based on impact – low, moderate, and high – and split into 18 different families. According to Blank (2020), the NIST SP 800-53 security control families are: Awareness and Training, Access Control, Audit, and Accountability Identification and Authentication, Configuration Management, and Contingency Planning Maintenance, Incident Response, and Media Protection, Personnel Security, Physical and Environmental Protection, Planning, Program Management, Risk Assessment, Security Assessment and Authorization, System and Communications Protection, System and Information Integrity, System and Services Acquisition.

2.8.2 ISM3

ISM3 stands for Information Security Management maturity model, and it enables an organization's information security maturity level to be divided into five categories of information security capability. The level of classification is determined by the form of controls and the type of technology enabled by the organization. These measures can be unavailable, ad hoc, repeatable, defined, managed, or optimized (Osamah et al., 2020).

The lack of protection and automatic controls in the company is referred to as the nonexistence maturity stage. The ad hoc maturity stage only employs automated security measures in extraordinary situations. Based on current cybersecurity understanding, the repeatable maturity level establishes automatic security controls. The maturity level defined starts by describing the security controls, techniques, and technologies needed to protect the organization. The managed maturity level is responsible for developing the technologies required to automate security measures. The optimized maturity level employs access control measures in order to protect the enterprise against both internal and external threats. Information security inspectors gather information on the technologies used, software, procedures, personnel, number of staff, and infrastructure to assess the security maturity level of the company (Osamah et al., 2020).

2.8.3 DNB

DNB (De Nederlandsche Bank) is an assessment framework designed to safeguard financial stability and thus contributes to sustainable prosperity in the Netherlands (Pijpers, 2015). To ensure that financial industries have sound information security process the DNB expects that financial organizations should have adequate procedures and measures should have to be in place to control Information security risks. To determine the continuity of IT and information security of an organization, DNB has created an assessment framework with which financial organizations can perform an assessment to evaluate the maturity of their information systems security. DNB information security assessment framework is developed based on COBIT v.4.1 and this framework includes 21 control objectives which are divided over 6 areas. These are strategy and policies, organization, people, process, and technology (Pijpers, 2015).

For defining the requirements first, the control objective from the DNB assessment framework is considered. Then each control measure is considered and based on the control measure specific requirements are defined. In this way, DNB performs a yearly risk assessment in which critical processes and controls are identified and it is evaluated how important each area and control measure of the DNB assessment framework for the organization's found in the Netherlands. Hence, financial organizations can determine which areas and control measures are more critical and which are less relevant due to the specifics of that organization when implementing the concrete requirements for each measurement metrics (Pijpers, 2015).

This assessment framework evaluates the information maturity level in the Netherlands and at the time many financial institutions likely still don't have all their controls at a maturity level of 3 (Toezicht, 2014). The following table 2.2 shows the DNB level of information security maturity.

Table 2.2. Overview of definitions of different maturity levels as defined by the DNB

Source: https://www.toezicht.dnb.nl/en/binaries/51-230767.pdf

Level	Control is: -	Criteria
0	**Non-existent** - No documentation. There is no awareness or attention for certain control.	
1	**Initial/ad hoc** - Control is (partly) defined, but performed in an inconsistent way. Individuals determine how they can carry out their tasks.	
2	**Repeatable but intuitive** - Control is in existence and is carried out in an organized and consistent manner, but in an unstructured way.	The execution of the control is based on an unwritten but standard procedure.
3	**Defined** - Control is recorded and carried out in a standardized and codified manner. Control execution can be demonstrated.	Formal control is available for any critical process. Critical process and controls are identified based on risk assessments. There is evidence of implementation of the control. Formal "test of design and operating effectiveness" constitutes evidence for level 3. The test of operating effectiveness should be done over an appropriate period which fits the risk profile.
4	**Managed and measurable** - The efficiency of the control is evaluated on a regular basis and improved when necessary. This assessment is documented.	Criteria for level 3 plus the following: - The periodic evaluation of the control is documented, including any identified action for improvement. The frequency of the periodic evaluation should be based on the risk profile. The frequency of this assessment should be at least annually.

5	**Optimised** - An enterprise-wide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time.	Distinguishing criteria are: Continuous improvement. Comparing control performance with market data of other enterprises. Advanced IT-support as workflow processing and integration.

2.8.4 SSE-CMM

The Systems Security Engineering Capability Maturity Model (SSE-CMM) was created with the goal of advancing security engineering because information security relates to the protection of data against a variety of threats in order to ensure business continuity, minimize risk, and maximize profitability and economic opportunities. Implementing an appropriate collection of controls, such as policies, processes, procedures, management cultures, and software / hardware operations, results in significant information security maturity. These controls must be established, implemented, monitored, reviewed, and improved as required to ensure that the organization's specific security and business goals are met. This can be done in conjunction with other aspects of business administration.

The SSE-CMM model and its associated assessment approach are currently available tools for assessing the capability of software vendors of security building materials, programs, and services, as well as directing organizations in identifying and developing their security project management. (Ferraiolo, 1998). SSE-CMM is an information security maturity model that investigates technology architecture to support organizational frameworks. It also instructs users on how to build controls for their software development and maintenance processes.

SSE-CMM's mission is to strengthen security engineering as an established, mature, and measurable discipline. The capability Maturity Model (CMM) for System Security Engineering (SSE) is a structure for designing processes such as formal and informal technical processes. It is divided into two parts: the model for process security approaches, programs, and organizations, the second is evaluation methods to understand the maturity process. The SSE-CMM includes 11 process areas. (Riadi, 2018). Administer security measures, determine impact, assess potential threat, assess challenge, assess weakness, and build protection argument are some of them.

coordination of security, monitor the security posture of the system, provide security feedback, specify security standards, and verify and validate reliability.

Through not promoting the process, SSE-CMM defines the basic characteristics of the organization's security engineering process that must exist to ensure successful security techniques. Specific or simultaneous, but take the industry's best practice (Riadi, 2018). This maturity evaluation model was used by assigning a score to each section of the application, ranging from 0 to 5, for each processing facility. The five Capability Maturity Levels describe increased operational maturity and are presented as follows:

- Level 0 indicates that not all of the fundamental practices are applied.
- Level 1 All of the core activities are carried out informally, which means there is no documentation, no standards, and everything is done on its own.
- Level 2 This identifies commitment preparation process standards as designed and monitored.
- Level 3 Standard processing has been carried out in compliance with the meaning.
- Level 4 is quantitatively regulated, indicating improved performance through process monitoring.
- Level 5 is continually improved, showing that the standard has been optimized and that the emphasis has been on adapting to the changes.

The maturity index is calculated using this model by taking the mean or consolidated value of the sample. The maturity model would be used to assess whether or not an issue exists. The maturity index is calculated from the value of the maturity level to achieve the maturity level in accordance with the table 2.3 below (Riadi, 2018).

Table 2.3. Maturity Level Assessment Criteria Index Source: Kurniawan and Riadi (2018).

Range	Descriptions
0 - 0.50	Non-Existent
0.51 - 1.50	Initial/ Ad Hoc
1.51 - 2.50	Repeatable but Intuitive
2.51 - 3.50	Define Process
3.51 - 4.50	Managed and Measurable
4.51 - 5.00	Optimized

In this research, the researcher is aimed to improve the maturity level of information security in the private banks of Ethiopia. This aids in determining the level of information security implementation and providing advice in terms of information security maturity level in banks. The study is primarily based on the ISO 27001: 2013 Standard and the Systems Security Engineering Capability Maturity Model (SSE-CMM) Maturity Level Assessment Model to achieve this target. This is due to the fact that ISO does not have assessment tools (Prayudi et al., 2016). The research mainly employs ISO 27001:2013 to regulate variables that are the information security assessment areas by involving the full security controls that are marked in section 2.6.2.

2.9 Information Security Maturity Assessment

The objective of assessing information security maturity is to provide strategic representation of the state of health of information security management (Narasimhalu et al., 2014). During the assessment organizations are categorized in to different maturity level. The Infosys Security Maturity Model (INFOSeMM), for instance, categorizes an organization into Inactive (Level 1), Reactive (Level 2), Streamlined (Level 3), and Proactive (Level 4) with respect to its current status (Narasimhalu et al., 2014). This classification is based on an analysis of information security maturity evaluations, which are divided into three categories: infrastructure, intelligence, and practices. The ratings assist the information security officer accountable for an enterprise's information security protection in assessing and reporting the corporation's information security maturity level to higher strategic top executives.

The information Security Maturity Assessment focuses on specific controls that protect critical assets, infrastructure, applications, and data by assessing the organization’s defensive posture. The assessment also emphasizes operational best practices for each control area, as well as the organizational effectiveness and maturity of internal policies and procedures. Based on the organization ’s objectives, sector, and maturity level, a security maturity evaluation can be customized to comply with several different established information security controls and frameworks.

2.10 Factors Influencing Information Security Maturity

According to Ryan (2006), only the allocation of resources to deploy preventive security efforts don't ensure the information systems security unless the support of top management. For consistent information security maturity, top management support is a crucial success factor. Upper executives must dedicate resources for both preventive and deterrence protection efforts in order to ensure efficient information security maturity. (Ryan, 2006). Equally important is an understanding of potential threats to information security helps to maximize the awareness towards keeping the information security protected. The majority of information security professionals have a good understanding of possible threats to the information system efficiency, as well as knowledge of effective precautions for each threat. However, due to the complex existence of rapidly developing security threats, most system users find it difficult to identify potential threats, which has a significant impact on the maturity of information security growth. (Thomson & Solms, 1998).

Schneier (2002) presented information security as a continuous process and proposed a gradual process approach to network security, and thus to information security, by reducing the possibility of unauthorized entry to each specified network access point. Similarly, Ferrarini (2001) has suggested five access points for continuous information security protection mechanisms are physical protection, authentication, access control, encryption, and security management. Ferrarini (2001) noted that an effective seal on any security access point was dependent on weighing the information the risk associated with the consequences of a given security breach. Within a business-computing environment, lack of user-level ISA (Information Security Awareness) hinders the maturity level of information security through inadequately protected or worse, undetected security breaches.

A growing number of data security vulnerabilities have been reported in recent years. Malware, virus, and power outage attacks, as well as minor errors with serious consequences, are all common occurrences. (Negash et al., 2019). Power outages, cyber-attacks, and hardware failures in the financial sector cannot be tolerated. Applications and systems go down any time and costing an organization time and money. Financial industries, like any other company, are vulnerable to threats that can damage their operations in various ways and jeopardize their survival. As a result, it is critical to establish and execute contingency plans in order to reduce the impact on their

information security efficiency, to be able to recover from disasters, and to mitigate the harm when a risk occurs.

2.11 Information Security in Financial Industries

To gain sustainable competitive advantage, financial sectors have incorporated information systems and related technology. In today's world, successful activity regulation and good organization approaches are linked to information quality management and monitoring. Financial industries are directly influenced by their reliance on information and technology services, processes, and the underlying mechanisms that form the foundation for these technologies due to the aspect of readily available information (Khan, 2015).

Procurement and selling products and activities, as well as transmitting properties and financial information over an interconnected medium, primarily the internet, is how financial companies conduct business. These transactions take place between banks, insurance companies, and customers. Mobile banking, internet banking, ATM service, POS (point-of-sale), bulk credit transactions, and other methods enable people to access their financial accounts in the modern world. As a result, people can pay for school tuition, DSTV (Digital Satellite Television), and plane tickets, as well as check their account balance and make any electronic payment the bank offers.

The business conducted using computers, telephones, barcode readers, credit cards, ATMs, internet banking, or other electronic appliances without the exchange of paper-based documents or physically moving to shop center. Information systems help financial institutions achieve their ultimate aim by providing the basis for conducting business in a simple and efficient manner. It allows you to serve a large number of customers at the same time. Even though the information system has benefits, it also has drawbacks when financial data is stolen or distorted by information security threats. Financial companies lose billions of dollars per year due to information security risks in the form of stolen money and loss of business. A company's marketing operations can be completely disrupted if protection is not adequately covered. Consequently, when a company falls to pay for cybercriminals in order to get back the encrypted data, may cause customers to worry about the security of their business transactions with the financial institution. As a result, if the company is considered to be vulnerable to information security risks, it could lose future business.

Due to reasonable complaints of financial analysts, investors, and creditors, such weakness will result in a reduction in the company's market value. (WALL, 2015).

Information security for the financial sector is a part of the information security model that is primarily applicable to the factors that impact information systems, such as data security and all other aspects of the framework. (Khan, 2015). Information security for financial security is the protection of information assets from unauthorized access, use, alteration, destruction, and deletion. The fast development of information technology allows people to access their mobile phones to conduct business. The underlying major obstacle in the advancement of information technology is that hackers can obtain information in the middle of a communications channel. (Bowrin, 2020). Hackers are individuals who commit data misinterpretation and data theft. As a result, weak financial information protection on web servers and technological devices creates vulnerability, which is then exploited by hackers.

2.12 Review of Related Works

Some academics have performed research on the maturity level of information system security in various organizations both locally and internationally. Table 2.4 lists the review of study that are linked with their respective researchers.

Table 2.4. Related works.

Tittle, Author & Year	**Objective of the study**	**Methodology & Technique**	**Key Findings**	**Observed gaps**
Eskatenafe and Tibebe (2017)	Investigating the maturity level of information security in Ethiopian banks	Surveying assessment techniques and DNB measurement technique	The maturity level of information security in Ethiopian banks are poor.	The research tries to evaluate with the DNB model which is country specific.
Assessment of Ethiopian public universities' information security maturity (Ejerssa ,2018)	To determine the extent of security maturity in Ethiopian public universities' information security implementation.	Both Qualitative and Quantitative approach has used.	The findings indicate that the information security maturity level in public universities is at infant stage.	The research has conducted to evaluate the information security of educational data which doesn't include financial transactions.
Assessment of maturity level of information security maturity using 2007 at hospitals in Addis Ababa, Ethiopia (Gera ,2019)	To measure the existing degree of information security management maturity in hospitals.	The study employed a hybrid strategy, as well as descriptive and inferential survey research methodologies.	According to the study's conclusions, the hospital's information security control environment is inadequate.	The study attempts to assess the information security maturity level of data discovered in hospitals. Specific to the sector.
Information System Security Management	The goal is to investigate the major issues	For data gathering, the study used a	The report suggests that new policies and	The study focuses on identifying

Challenges in Kenyan Higher Education Institutions, (Bichanga & Obara, 2014)	confronting information system security management in higher education systems.	descriptive survey, as well as qualitative and quantitative research approaches.	procedures be implemented to guide information system security.	information security management difficulties rather than evaluating security maturity.
A Framework for Measuring Information Security Performance at Various Levels of Maturity (Rosmiati & Yudi, 2016)	Determine the level of information security in the organization in order to make recommendations for improvements in information security management.	A questionnaire and a qualitative research approach were delivered to the 14 respondents that were sampled.	The results indicate that the Bureau of Information Advances in technology information security maturity level is at level 2. This falls short of the standard required.	The sample space is restricted, and the study approach is oriented on information security management systems.

As it is presented in table 2.4, different researchers have tried to measure the information the security maturity level of an organization through the sectors are different. Hence, they have identified security gaps in relation to international standards.

Descriptive research by Bayu and Beshah (2017), is conducted on the Information System Security maturity level of the banking industry in Ethiopia. The goal of the study was to conduct a descriptive analysis of information security maturity levels in Ethiopian banks in order to understand the situation and identify difficulties, bottlenecks, and factors that influence information security management maturity levels in banks. This research undertook using

quantitative analysis of information security management in the financial sector. The study seeks to provide a complete and analytical evaluation of the situation to determine the maturity level of Ethiopian banks.

To identify the level of information security maturity level the research collects data from 18 banks and evaluate it with DNB (De Nederlandsche Bank) information security maturity level framework. Which is country-specific. And the study recommends that future research would be conducted in well-placed to focus on benchmarking information security maturity level in this area. At the time of the research, the study identified that there is no information security framework or standard used by banks, and there is no regulatory framework enforced from the banking regulatory body as well to protect the information from any aspects of the threat. Finally, the study suggested that adopting an information security framework will not be enough to ensure information security and not adequate to close the security gap, instead of assessing information security maturity level periodically helps to improve the information security protection mechanism.

Another researcher Ejerssa (2018), and Gera (2019), carry out an information security maturity level gap analysis for Ethiopian public universities and hospitals, respectively. Their study's goal was to evaluate the Information Security Maturity Level (ISM) norms of higher education and hospitals, and to propose and recommend the best practices standing from international information security protection standards. However, the study doesn't include financial sectors and their feature research recommendation was pointing to measure the information security maturity level of other industries and financial sectors is one of the main organizations placed at risk unless its maturity level has grown as the technology grows up, since measuring maturity level is not one time work regular monitory is recommended.

Bichanga and Obara (2014), seeks to study the issues that information system security management faces in Kenyan higher learning institutions. The study employed a descriptive survey approach, with the populations addressed being information systems project managers, administrators or senior management, and other system users in critical departments. employed a systematic sampling technique. SPSS descriptive statistics were used to analyse the data. The factor analysis methodology was used to determine the primary difficulties that affect an institution's information system security management. Pearson's Chi-Square was employed to

examine the correlations between frequency distribution. Finally, the study recommends that new rules and procedures regulate information system security, as well as that university administration create habits of demonstrating compliance or reduce the factor that influence quality of the information and identifying strategic remedies. Regarding this research scientific and most recent information of threat and the capacity of information security maturity level has to be identified.

An effective information security development and implementation requires well-designed policies and procedures to ensure inclusive understanding of the current state of security follow up and monitoring. In the past years, many researchers conduct their study towards on resolving different information security-related risks. Among those researchers most used ISO information security standard as a benchmark to assess the information security practices of different kinds of organizations. Currently there are various information security standards are used around the world which includes mostly utilized standards like COBIT, ITIL, DNB, PCI-DSS, BS7799, etc. among those standards, ISO27001:2013 gives inclusive and most acceptable information security standard for different countries and organizations. This research adopts the ISO 27001:2013 information security standard with its management practices of selection, implementation and monitoring of controls are taken into consideration that allows the organization to protect its information system and related properties from security risks.

The study aims to fill is by introducing globally acceptable information security guidelines, establishing overall security requirements based on ISO 27001:2013, and leading in a higher and safer level of information security maturity for Ethiopian private banks. As a result, information system protection has been guaranteed in terms of confidentiality, availability, and integrity. Various researchers have based their research on the ISO 27001 information security standard. YEMANE, (2018) conducted a study on the information security management system for Ethio telecom using ISO 27001:2013, which is one of the numerous reviewed relevant works under chapter two. Similarly, the ISO 27001:2013 information security standard is used to define variables that are important focus areas for his research.

The related works show that the information security maturity have not been sufficiently addressed in the case of the private banks in Ethiopia. Benti and Julius (2013) iterated that more secured information security management in an organization is considered a good approach in increasing the organizations effectiveness, efficiency, performance and decision-making capability. As a

result of the nature of complex and competitive information development, it is necessary to examine and analyse potential risks that prevent the organization from reaching a high level of information systems security maturity.

Measuring the security maturity level of information systems with standardized metrics increases the ability to recognize and manage information security safety. Therefore, in order to protect information from various security threats, organizations need to understand their information system security maturity level requirements on a regular basis. As a result, this study was conducted to address certain issues in the study field.

2.13 Summary

The chapter was mainly focused on reviewing pieces of literature which are related to maturity of information systems security in an organization. More importantly popular information security standards and information security maturity models are discussed, factors influencing Information Security Maturity are presented, related works are reviewed and synthesis is made to make sense out of them in order to show the research gap this research is aimed to fill. The next chapter deals with the research design and methodology.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter presents the research design and methodology of the study. In more detail, in this part, the researcher outlines the research strategy, research method, research approach, methods of data collection, selection of the sample and study setting, research process, type of data analysis, and the validation and reliability. These chapter gives a detailed explanation for the instruments that is used for data collection also describe the procedures that were followed to carry out this study. The components involved in conducting this research from the total population to the sampling techniques used for the questionnaire are explained. Finally, this chapter provides a detailed explanation of the selected mode of the analysis used and data validation and reliability techniques used.

3.2 Research Design

The Research design defines as the method and procedure for collecting, analysing and, interpreting the overall study to be conducted in one research (Akhtar, 2016). The research design refers to the overall strategy that the researcher takes place to integrate different components of the study in a comprehensible and reasonable way. Thus, it ensures the researcher effectively address the research problem by constituting the data collection, measurement techniques, and the analysis of data. Hence, the basic function of a research design is to ensure the evidence obtained and the data collected through the study allows to effectively address the research problem logically and as explicitly as possible.

The research design is about the structure of the study and it holds every element of research together. According to Akhtar (2016) Research design stands for advanced planning of the technique to be adopted for collecting relevant data and the techniques to be used in the analysis. As Boru (2018) cited in the study by Robson (2002) states, there are three possible forms of research design. Those are: exploratory, descriptive, and explanatory. The classification is based

on the purpose of applying to different study areas. Among those research designs, this study employs a descriptive research design.

The descriptive research aim is to accurately and systematically describe the population, situation, or phenomena that occurred and can answer what, where, when, and how questions (McCombes, 2019). Unlike other research design methodologies, descriptive research design can use a wide variety of research methods to investigate variables and the researcher doesn't control or manipulate any of the variables, but possible to observe, investigate through different techniques, and can measure them. Descriptive research design is more appropriate and can be applied when the research aim is to identify the characteristics, frequencies, trends, and categories (McCombes, 2019).

Thus, in this research, the researcher employed a descriptive research design since this design allows the researcher to describe the situation or case under in this study. It is a theory-based design that is created by gathering, analysing, and presenting the final result of collected data. Descriptive research is used to obtain information concerning the current status of the situation and to describe what exists with respect to variables or conditions in a specific study area (Akhtar, 2016). The goal of descriptive research is to describe a phenomenon and its characteristics.

3.2.1 Research Approach

The research approach is a plan and procedure that consists of the steps of broad assumptions to detailed methods of data collection, analysis, and interpretation (Creswell, 2013). Hence, an approach used to implement in research is a method to get information from the sample. Cresswell (2009) describes the importance of illustrating the research approach as an effective strategy to increase the validity of the research.

This research uses quantitative data collection for measuring the information system security maturity level of the private banking industry. The research approach believed that helps to understand the main gap in the study area.

An organization's information system security maturity resides mostly on the technical employees of an organization besides the technology employed. Thus, the researcher found it important to collect data using a quantitative approach from sampled employees using a questionnaire to meet

the research objective. Also, According to Almalki (2016). The researcher uses this approach to better understand in-depth insights into a problem and collect data to get core measurement values on the actual information system security areas.

3.2.2 Research Strategy

A research strategy introduces the main components of a research project like the research topic area and focuses point, among those case study research strategy focuses on an in-depth investigation of a single case (e.g., investigate one organization) or a small number of cases. Research strategy mainly referred to the information which is gathered from different sources and through the use of different types of data such as quantitative surveys, and analysis of documents.

Case study research allows a composite and multifaceted investigation of the issue or problem (Creswell, 2013). The research strategy is the procedure and plans that the researcher follows to monitor and execute the study (Thomas, 2001). The case study research design is more important to check and evaluate the actual working framework to comply with the model or theory designed for a specific fact (Ebrahim, 2018). Standing from this fact researcher plan to implement case study research on descriptive research. The reason for taking data from those working at different levels of private banking was to have an in-depth understanding of the issue under study.

Therefore, survey tools are often used to gather data. In this research, the data collected through a quantitative approach and analysed quantitatively, using frequencies, percentages, averages, or other statistical analyses to determine the maturity level of an information system security for sampled private banks.

3.2.3 Study setting

The research setting comprises the location, environment, social and cultural behaviour of the study location (Given, 2008). Therefore, this research is conducted on selected four banks headquarter sites located in Addis Ababa and IT/MIS department employees, who is responsible for information system security-related works.

3.2.4 Case selection

The sample is a part of objects taken from a population, which is considered to be representative of the population. For this study, the researcher employed stratified probability sampling to select four banks among the available 19 banks[2] according to the data retrieved from the national bank of Ethiopia website. Those banks are grouped into four groups (strata) based on their high-profit achievement 2019/2020 fiscal year. The banks are grouped into four-layer and the researcher picks one bank from one stratum.

3.2.5 Study participants

A research participant is an individual that participates in research and expected as important to collect data from the sampled that helps to answer the question under this study. The study sample members in this study were chosen based on their specific link with the topic under study, as well as sufficient and relevant professional expertise in the field of information security. The sample objects are nominated based on their knowledge and position for the study area. The target population for this study is that of the overall management information system department employees located at the head office of each sampled private bank.

3.2.6 Sampling Design and Sampling Techniques

In order to do quantitative study, for getting participants' replies to the questionnaire survey, it is necessary to design a sampling that represents the theoretical demographic population (Given, 2008). For the research to be done, sufficient data from a representative sample of the population is required. Participants for this survey are personnel in the information service management and management information system division at head quarter, because the private banking sector is broad and has a wide area coverage all over the country and the information system has managed centrally. The questionnaires for the survey are written in English.

From the sampled four private banks using stratified probability sampling Bank A, Bank B, Bank C, and Bank D placed in order of their highest to lowest profit attainment, from A to D. In addition, each private bank's participants were chosen, and the 110 questionnaire was distributed to respondents using a simple random sampling method. This is in the ratio of Bank A receive 30

[2] https://nbebank.com/banks/

questionnaires, Bank B receive 30 questionnaires, Bank C receive 25 questionnaires, Bank D receive 25 questionnaires.

3.3 Analytic Tools and Techniques

Regarding the analytical tools used in this research, since the primary data has collected through direct information gathering using questionnaire from the target group of information system security and related departments of each sampled private banks and secondary data has going to be collected from document analysis and literature review on the study area. This is because information system security experts, system and database admins and higher officials responsible for system security are responsible for ensuring the system has worked fine through protected and secured way by following the required policy, procedure, and techniques, etc.

The data collected through primary and secondary are evaluated based on the ISO/IEC27001:2013 information security management system requirements and the assessment of measuring the maturity level has conducted based on the SSE-CMM. The main reason to use these tools is ISO doesn't have its own security maturity measuring technique and ISO/IEC has agreed and accepted standards internationally and it has updated regularly. ISO 27001 has 14 control objectives (Georg, 2013).

SSE-CMM describes and targets the essential characteristics of the information security engineering process that have to be existed to ensure a good information security maturity level. The SSE-CMM is categorized into two parts which are process and maturity levels. The process category defines the security engineering process that has to be accomplished, and the maturity levels are designed to advance security engineering as a defined, mature, and measurable discipline to achieve the highest level of how the information security process accomplishes its goals. Generally, the SSE-CMM model has been designed to improve the existing system security engineering. It has 6 capability levels which provide a logical and structured methodology for improving how work is performed. SSE-CMM approach was employed by assigning a score to each process area ranging from 0 to 5 for each given process. (Supriyatna, 2014).

The ISO/IEC 27001 information security control goals are coupled with the SSE-CMM in this study and used as a combined information system security maturity assessment technique. The

main reason to link this model and assessment tool is they have designed with similar goal of ISM. The main reason for linking this model and maturity assessment tool is that they were created with the same purpose in mind as ISM. The SSE-CMM model identifies the features of a company's security engineering process that must be available in order to assure good security engineering (Riadi, 2018). The SSE-CMM is a generally acknowledged and internationally recognized model for measuring and evaluating the maturity of security processes and controls within an organization.

The use of an SSE-CMM method can facilitate the development of a continuous improvement approach to ISM and the attainment of greater levels of competence and capability in ISM processes and procedures. Furthermore, SSE-CMM process areas can be used by the business to optimize common activities and align processes in order to establish an efficient ISM strategy. As a result, ISO/IEC 27001 information system security requirements are mapped to the information security domain and each process found inside it.

3.4 Research Techniques

The research techniques are the plan of a framework for the study. It is used as the main guideline to identify what kind of data has required and what kind of methodology going to be used to collect data and analyse the data collected through different data collection instruments. This is conducted to find answers to the research questions. According to (Akhtar, 2016) a descriptive type of research are those studies that are concerned with identifying and describing the current existing trend of a particular organization. Here in this research, the researcher going to implement a descriptive kind of research that tries to investigate the maturity level of information system security capability in the case of private banks of Ethiopia.

The research technique is the significant part of a study because it helps to find the way on how to achieve the general and specific objectives of the research, the data collection instrument, the data analysis and presentation. Which collectively works together towards answering the research question.

3.4.1 Data Collection

Quantitative research approach was used to collect data. In general, data were collected through questionnaire survey and document analysis. The primary data was collected through questionnaire. Whereas the secondary data was collected through document analysis.

Secondary data was gathered through document analysis and a review of the literature in order to better understand the actual information system security maturity level of Ethiopia's private banking sector. Finally, expert view and critical analysis was conducted to get more insight and understanding to the actual data.

3.4.1.1 Questionnaire

The questionnaire is utilized as the primary data collection method in this research, and it is derived from (Gebrehiwot, 2018; Ejerssa, 2018). Which is attached in appendix B consisted of two parts containing the personal information in general, as well as the current state of information systems security.

The questionnaire assists in the evaluation of ISO/IEC 27001's 14 security areas and determining the maturity level of information security, as well as the important elements that influence the performance of the information security maturity level in Ethiopian private banks. The items in the questionnaire are primarily based on the ISO 27001:2013 information security management guideline.

3.4.1.2 Document analysis

For this research, the researcher reviews the information security management policy and procedure documents if the sampled bank formulates and conduct its day-to-day activity to protect the organization, from security threat based on the designed document. The researcher reviews the document if it is prepared according to the international information security standard (ISO 27001:2013). This kind of document analysis helps the researcher in determining the validity and reliability of the questionnaire response.

3.4.2 Data Analysis Strategy

Due to dynamic nature of information technology, there is a crucial and adequate information security maturity level measurement has required (Georg, 2013). In this study the data collected is analysed using descriptive analysis. Statistical analysis is employed to quantitatively analyse the data from the questionnaire survey. Hence quantitatively collected data was analysed using SPSS version 25.0.

In recent researches, to conduct and find out the information security maturity level organizations has better to use an ultimate measuring tool and assessment technique like ISO 27002 using SSE-CMM (System Security Engineering Capability Maturity Model) check list (Riadi, 2018). According to Prayudi et al., (2016) the SSE-CMM consists of two categories. The first one is model for process security technique and the other is assessment methods to know the maturity process. This study is mainly conducted based on ISO/IEC 27002: and maturity level evaluation tool of SSE-CMM. This is due to the ISO's lack of assessment methodologies. The findings from those two methodologies are thought to produce a more compressive conclusion to suit the study's purpose.

3.4.3 Validity and Reliability

According to (Creswell, 2009), the real situation in a study exists when scores are both reliable and valid. Validity is concerned with whether the measuring instrument measures the behaviour or quality that it is intended to measure and is a measure of how well the measuring instrument performs its function (Maslakci, 2020). To ensure this, the score from the measurement instrument have to generate meaningful and valid result. Hence the data collected should be free from measurement error and measuring scale. Therefore, to ensure reliability and validity the researcher follows ISO/IEC 27001 international code of practice for information security standard.

In order to determine the validity of measuring instruments different kind of validity have been suggested on the literatures. Several methods have been proposed for determining content validity. Among them taking expert opinions and statistical methods are the two most frequently applied methods. In this study the researcher appointed expert opinion and experts are appointed to evaluate each expression.

Even if the questionnaire was based on related research. It is necessary to assess the necessity of each question in order to omit misunderstandings and to ensure that there are no ambiguities or errors on the inquiries. As a result, the questionnaire was delivered separately to the study's advisor, who thoroughly evaluated and modified them. Furthermore, security managers from chosen private banks are invited to analyse and check all aspects of the presented questions, and these experts provide good feedback with some small adjustment's suggestions.

3.5 Chapter summary

The chapter presented about the research design and methodology content of the study. The design and methodology techniques are briefly described on the basis of how it can be more useful to answer the research questions and meet the objectives of the study. This research uses the quantitative research approach to collect data from the participants, defines the research strategy, detail describe the study setting, indicates the sampling techniques used and population of the study. Also, the research techniques and methodologies which enables the researcher to present the data collection instruments, procedure, source and presentation. Finally, the analysis and data presentation strategy of the study has discussed were the researcher going to analyse the quantitative data using SPSS version 25 and present graphical and tabular information's. The research evaluates the actual information systems security approach towards the international information systems security standard which is ISO/IEC27001:2013 information security management systems requirement and SSE-CMM system security maturity level assessment tool are used to indicate the maturity level of specific sampled private bank.

CHAPTER FOUR

DATA PRSENETATION AND ANALYSIS

4.1 Introduction

This research yielded h quantitative information. The chapter includes three main parts. The first section is about analysing and presenting quantitative data. The information security maturity level has measured on fourteen information security requirement criteria based on ISO27001. Information security policies, human resource policy enforcement, asset management regulations, access control authentication, cryptography regulations, physical and environmental security policies are all included and operations security policies, system acquisition, development, and maintenance, supplier relationships, information security incident management, information security aspects of business management process, information security incident management.

To deal with this, a hundred and ten questionnaires were distributed to the respondents. The questionnaire was developed in the online google form and distributed to the respondents through email and skype. Among the total of 110 questionnaires, 93 of the respondents completed and returned the questionnaire, while two respondents did not return it by answering the majority of the questions. This indicates that 84.5% of the questionnaires were returned, and 91 of them are used in this analysis. Responses were taken as valid for further data processing if one of the questions has answered from each of the control objectives. The data was gathered and checked to see if there were any missing or inconsistent answers from the selected questionnaires. Having followed the validation of the questionnaires, the collected data were analysed using SPSS version 25 to further investigate the results and make recommendations based on the findings.

To present the frequency and percentage the researcher used tabular format since a frequency table is one of the most common methods for presenting descriptive statistics, making it much easier to interpret and understand the data presentation's result. Finally, the essential and necessary specifications of ISM are described, along with a detailed explanation of its components.

4.2 Quantitative Data Presentation and Analysis

Under this subsection, the respondent's demographic characteristics, organizational information, and maturity level assessment is analysed from the data collected and presented as follows. The first part contains the data of sampled individuals' personal information, qualification and years of experience. While the second part designed to evaluate the security control objectives into 6 levels from 0 - 5, a six-point scales are, "0" None, "1" Initial, "2" Not-Defined, "3" Defined, "4" Managed "5" Optimized is used. The first section of the questionnaires was aimed to collect respondent information and their position on the organization, while the second section was aimed to collect data on actual information system security maturity level.

4.2.1 Respondent Demographic Characteristics

The demographic data introduces the respondent information from the division of information system department of the four sampled Ethiopian private banks. The demographic variables used in this study include respondent's job position, years of experience working on the area and educational status of the respondent.

4.2.1.1 Respondents Job Tittle Response Rate

In terms of the respondents' job position (Table 4.1) shows that 10 (11.0%) of the respondent are Application Administrator, 6 (6.6%) are in a position of Storage and Server Administrator, 5 (5.5%) of the respondent are Core Banking Operation Specialists, 9(9.9%) are in a position of IT Service Desk Operation, 9 (9.9%) are in System Development Engineering, 8 (8.8%) of them are IT Security Specialists, 6 (6.6%) are in a position of Network Security Administrator, 12 (13.2%) are in a position of Service Management Administration, 7 (7.7%) are in a position of Security Operation Officer, 8 (8.8%) of them are Database Administrator and finally 11 (12.1%) of respondents are missing the job position they are working on.

Table 4.1. Distribution of respondents by Job Position.

Respondent Job Position		
Job Position	Frequency	Percent
Application Administrator	10	11.0

Storage and Server Admin	6	6.6
Core Banking Operation Specialist	5	5.5
IT Service Desk Operation	9	9.9
System Development Engineer	9	9.9
IT Security Specialist	8	8.8
Network Security Administrator	6	6.6
Service Management Admin	12	13.2
Security Operation Officer	7	7.7
Database Administrator	8	8.8
Total	80	87.9
Missing Value	11	12.1
Total	91	100.0

4.2.1.2 Respondents Qualifications

The analysis took into account the respondent's educational background, as seen in table 4.2. The majority of the respondents have a bachelor's degree, with a percentage of 74% and those who have a master's degree are 26% of the total respondents. This indicates ¼ of the total respondent have achieved master's degree and the rest of them have minimum bachelor degree this indicates that respondents were well-educated and hence they are capable of answering the research question with confidence. Also, respondents with appropriate qualifications were also included in the survey.

Table 4.2. Distribution of respondents by Educational Status.

Educational Status		
Educational Status	Frequency	Percent
Diploma	0	0
Degree	67	74
Masters	24	26
PhD	0	0
Total	91	100

4.2.1.3 Respondents Experience

The respondents were asked how long they had worked at the bank, and table 4.3 demonstrates this point. This question was answered by all 91 respondents, and the majority of them, 37 (41 %), have work experience ranging from six to ten years. 28 (31 %) of the respondent are found in experience range of three to five years. 16 (18%) are working for two years or less. 9 (10%) of respondents have eleven to fifty years of experience, with the remaining 1 (1%) having worked for more than fifty years. This implies that the survey included respondents with a wide range of experience in the private banking sector.

Table 4.3. Distribution of respondents by work experience

Work Experience		
	Frequency	Percent
2 years or less	16	18
3- 5 years	28	31
6 - 10 years	37	41
11 - 15 years	9	10
More than 15 years	1	1
Total	91	100

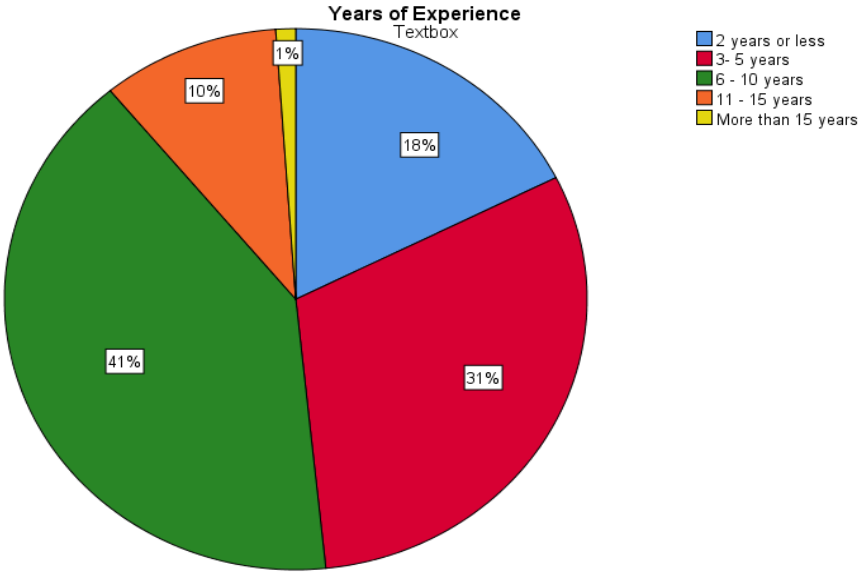

Figure 4.1. Distribution of respondents by work experience

4.2.2 Organizational Information

Respondents are asked to describe and indicate details about their organization in this subsection. As a result, the elements included in the analysis of the organization's behaviour against information security are the information security management standard they use, the institution's compromise background, and the presence of dedicated professionals for information security management and incident response, as well as the ongoing training and enhancement of information security expertise for employees. As a result, the following section discusses the specifics of the information gathered.

4.2.2.1 Information Security Management Standard

The respondent was asked whether their organization has a structured information security management standard or framework that they adopt on a daily basis. As shown in table 4.4, the majority of 64 (70.3 %) of respondents confirm their company has an information security management standard, while 7 (7.7 %) of respondents say “No” to the ISM standard and 20 (22.0 %) of employees “Don't know” whether their organization has an information security standard.

Table 4.4. ISM Standard usage in the institution

Use Information Security Standard		
	Frequency	Percent
Yes	64	70.3
No	7	7.7
Don't Know	20	22.0
Total	91	100.0

The sample selected respondent was asked to specify which international security standard or system their organization uses, and in this question, the most common information security management standards are listed with checkboxes to choose from: ISO, ITIL, and COBIT. Some organizations use two or three security standards concurrently, while others use only one information security standard. According to table 4.5, 34 (37.4 %) of participants say their information security standard is ISO, while 28 (30.8 %) say they do not really.

Table 4.5. ISO information security standard

ISO information security standard		
	Frequency	Percent
Yes	34	37.4
No	28	30.8
Total	62	68.1
Missing	29	31.9
	91	100.0

Whereas the table 4.6 indicates the ITIL information security standard, 28 (30.8 %) of respondents say "Yes" and 37 (40.7 %) say "No".

Table 4.6. ITIL information security standard

ITIL information security standard		
	Frequency	Percent
Yes	28	30.8
No	37	40.7
Total	65	71.4
Missing	26	28.6
	91	100.0

The final information security standard in the choice was COBIT, and according to the table 4.7 below, 17 (18.7 %) of respondents say “Yes,” while 48 (52.7 %) say they do not use COBIT as their ISM.

Table 4.7. COBIT information security standard

COBIT information security standard		
	Frequency	Percent
Yes	17	18.7
No	48	52.7
Total	65	71.4
Missing	26	28.6
	91	100.0

Finally, respondents were asked an open-ended question to list out their information security standard if it was not specified on the above standards and as shown in table 4.8. 63 (69.2 %) of participants say "No" and 2 (2.2 %) say "Yes" on using other information security standards.

Table 4.8. Other information security standard (except ISO, ITIL and COBIT)

Other than the listed Information security standards		
	Frequency	Percent
Yes	2	2.2
No	63	69.2
Total	65	71.4
Missing	26	28.6
	91	100.0

4.2.2.2 Compromise with Information Security Attack

Table 4.9 shows the results of a survey that asked study participants whether their company had ever been harmed by information security issues in the past few years. The majority of respondents, 59 (64.8 %), say “Yes” to compromise, while 17 (18.7 %) say there was no information security attack. Whereas 15 (16.5 %) of participants are unaware of information security threats to their organization.

Table 4.9. Compromise with information security attack

Compromise with Information Security attack		
Compromised	Frequency	Percent
Yes	59	64.8
No	17	18.7
Don't Know	15	16.5
Total	91	100

Respondents who replied "Yes" for information security compromise were asked to categorize the type of the security attack as internal, external, or both. This question was answered by 59 participants. 24 (40.7 %) of respondents said there was an internal security attack, 13 (22.0 %) said

the attack came from outside, and 22 (37.3 %) said all types of attacks had occurred at their institution.

Table 4.10. The source of information security attack

From where the attack emerges		
	Frequency	Percent
Internal	24	40.7
External	13	22.0
Both	22	37.3
Total	59	100

4.2.2.3 Information Security Personnel

Since information security is broad and requires supervision, respondents were asked if their company has a dedicated employee who is responsible for information security management and controlling any information security matters. According to the table 4.11, the majority of 84 (92.3 %) of respondents said "Yes." 4 (4.4 %) of respondents say “No” to dedicated information security employees, and the remaining 3 (3.3 %) do not know if there is a dedicated employee on the information security management division.

Table 4.11. Information security dedicated personnel

Information Security personnel		
	Frequency	Percent
Yes	84	92.3
No	4	4.4
Don't Know	3	3.3
Total	91	100.0

Based on the information provided above, respondents were asked to indicate whether information security staff are getting security-related training. As shown in table 4.12, the majority of respondents (43 (47.3 %) say they are taking training sessions, while 17 (18.7 %) say they are not, and 27 (29.7 %) are unaware of the training on security-related issues.

Table 4.12. Attend security related trainings

Did they attend security-related training		
	Frequency	Percent
Yes	43	47.3
No	17	18.7
Don't Know	27	29.7
Total	87	95.6
Missing	4	4.4
	91	100.0

4.2.3 Maturity Level Assessment

The maturity level evaluation focuses on monitoring the organization's growth and progress culture in filling gaps to move from the current state of information security protection to the identified goal. The SSE-CMM has provided six tires of level as a guide that helps organizations to understand the characteristics of their information security maturity level. Hence, as discussed in Chapter 3 of this report, the international standard for information security requirements (ISO/IEC 27001) does not provide organizations with a framework to assess the progress and maturity level of the information security process capabilities.

Therefore, an information security maturity model is expected to assess the capabilities of information security protection. The key goals of the maturity model are to define a baseline from which to begin strengthening an organization's security posture while implementing SSE-CMM. Some frameworks do not have a maturity model. they employ other information security maturity models, such as ISF MM, ONG C2M2, and SSE CMM for system information security standards that do not have a maturity model, such as ISO 27001. (Almuhammadi, 2017).

The researcher conducts this research to investigate and identify the current information security maturity level of Ethiopian private banks from among 16 private banks by grouping them into four strata and selecting one from each stratum. However, for the first four private banks chosen, two of them do not consider or entertain cooperation letters from any researcher unless he or she is a member of their organizations. As a result of communicating with advisor, those who are unable to accept recommendation letters have been replaced by other private banks by their stratum classes.

To determine maturity level, a questionnaire was collected online using a Google form, exported to a csv format, and analysed using Microsoft Excel software. The data was analysed using SPSS V.25 to reflect the collected data as frequencies, means, and percentages in a significant measure. Fourteen areas of information security were discussed, along with their stages of maturity. The following section summarizes the results for each security control objectives.

4.2.3.1 Maturity Level Result and Analysis

The maturity level for each information security control objective, domain, or segment was determined by categorizing the responses into 6-point levels ranging from 0 to 5. The interpretation of the respondent values is as follows. 0- non-Existing 1- Initiative 2- Repeatable yet Intuitive 3 – Defining 4 – Managing 5 – Optimizing. As a result, each questionnaire's respondent evaluation was collected, and Microsoft Excel software calculated the average (Mean) of the responses for each control, domain, or category. The average result produced represents the degree of information security maturity of private banks in each of the ISO 27001 Information security management control objectives.

Table 4.13 shows the mean of the outcome descriptions obtained by the respondents per clause. The maturity index is the outcome of determining the level of information security maturity by calculating the importance of the maturity level ranging from 0 to 5. Since information protection is linked to the privacy of the institutions, any one of the sampled bank names are not revealed in this study, and the data filled from various private banks is collected, then stored in one, and analysed. SPSS software is used to generate the descriptive analysis and frequencies. The aggregate outcome of the study to determine the mean value of information security controls in Ethiopian private banks in comparison to the sampled four banks is 2.45, and the last expected information security maturity level is 5. (Optimized). Based on this instance, we may infer that the maturity level of a private banking institution is second, i.e., repeatable but intuitive.

Table 4.13. Maturity level summary for each control objectives

Clause	Control Objectives	Index	Level
5	Organization of information security	2.47	2
6	Human resource security	2.45	2
7	Asset management	2.34	2

8	Information security Policy	2.41	2
9	Access Control	2.57	3
10	Cryptography	2.19	2
11	Physical and environmental security	2.73	3
12	Operational security	2.48	2
13	Communication security	2.37	2
14	System acquisition, development and maintenance	2.45	2
15	Supplier Relationships	2.57	3
16	Compliance	2.59	3
17	Information security incident management	2.32	2
18	Information security aspects of business continuity management	2.29	2
Average		2.45	2

As it can be seen from the above table for annex A.9 (Access control), A.11 (Physical and environmental security), A.15 (Supplier relationship) and A.16 (Compliance) the average allocated to their equivalent score reaches the maturity level of 3 which is (Defined) and for the rest of control objectives the mean value indicates score level 2 (Repeatable but intuitive) of information security maturity level. This is because the System Security Engineering Capability Maturity Model (SSE-CMM) classifies the score as ‘Repeatable but intuitive,' with a range of 1.51 to 2.50 whereas if the score ranges from 2.51 to 3.50 entitled with ‘Defined’. Figure 4.2 depicts the maturity level of information security for private banks in each of fourteen areas derived from ISO 27001:2013. The assessment scale indicates that the organization has a score of less than three in all information security maturity metrics, as seen in the figure 4.2.

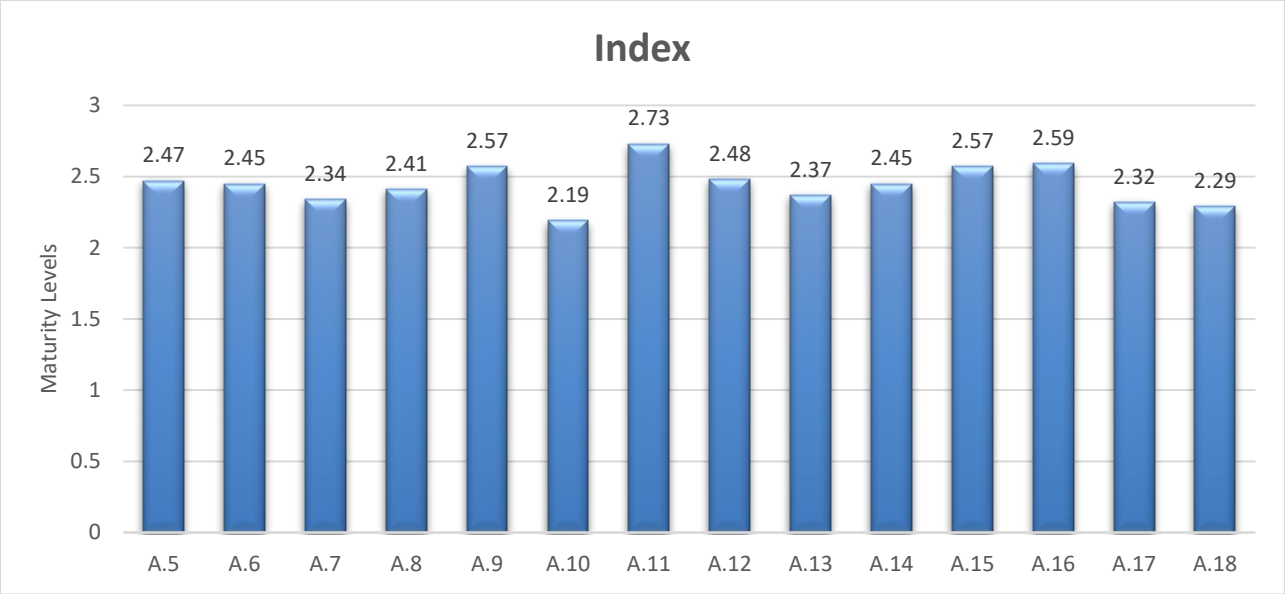

Figure 4.2. Maturity level score per each security area

4.2.3.2 Maturity Level Per Banks

The level of information system security maturity among the sampled private banks is also examined. Bank A, Bank B, Bank C, and Bank D were ordered in sequence of highest to lowest profit achievement from the sampled four private banks using stratified probability sampling. As can be seen in the figure 4.3, the average maturity level for the first high profit bank is 2.50, the average maturity level for the second category is 2.48, the average maturity score for the third category sampled bank is 2.39, and the average score result for the final category is 2.43.

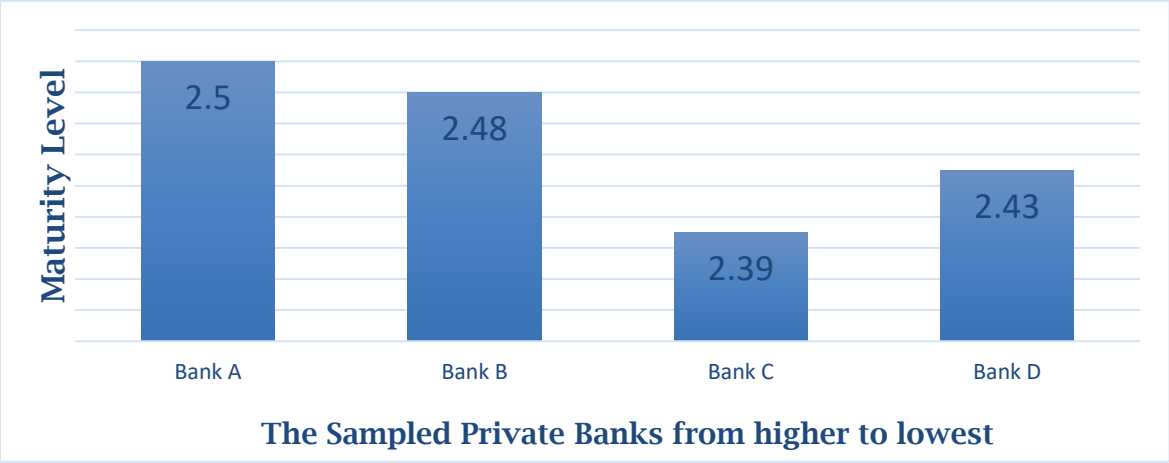

Figure 4.3. Maturity level score per bank

From the quantitatively collected data the study finding shows that Bank A, Bank B, Bank C and Bank D have on maturity level of 2 based on the SSE-CMM Maturity Level Assessment Criteria since it says from if maturity metrics range between 1.51 to 2.50 the maturity level is Two which is Repeatable but Intuitive. For all information security areas, the maturity level value has categorized by the range of SSE-CMM maturity level assessment criteria which is described on section 2.8.4 of this research.

Thus, the study finding shows that the sampled private banks information security maturity level has shown no significant difference. But there is some difference on their attention towards the information system security management criteria of the ISO 27001. Thus, Bank A has achieved the upper score for the maturity level on A.8, A.11 and A.16 whereas the lowest maturity level score on A.5, A.10 and A.17. Bank B score high on A.11, A.15 and A.16 whereas low score on A.13, A.14 and A18. Bank C score high maturity level on A.9, A.11 and A.16 whereas score low maturity on A.8, A.10 and A.18 and finally Bank D score high maturity level on A.5, A.11 and A.14 whereas score low maturity on A.7, A.17 and A.18. Table 4.14 shows the detailed maturity level results for each bank based on the ISO27001 annex.

Table 4.14. Maturity level of each bank per each ISO 27001 security area

Banks from Four Different Group	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18	AVG
Bank A	2.23	2.42	2.5	2.8	2.58	2.1	2.69	2.6	2.52	2.67	2.52	2.71	1.99	2.61	**2.50**
Bank B	2.51	2.51	2.47	2.4	2.57	2.37	2.79	2.41	2.2	2.29	2.77	2.64	2.44	2.34	**2.48**
Bank C	2.44	2.41	2.41	2.01	2.66	1.99	2.8	2.32	2.31	2.23	2.49	2.6	2.54	2.18	**2.39**
Bank D	2.7	2.44	1.97	2.41	2.45	2.42	2.63	2.58	2.58	2.59	2.49	2.41	2.31	2.01	**2.43**
Average Per Security Controls	**2.47**	**2.45**	**2.34**	**2.41**	**2.57**	**2.19**	**2.73**	**2.48**	**2.37**	**2.45**	**2.57**	**2.59**	**2.32**	**2.29**	***2.45***

4.2.3.3 Maturity Level Gap Analysis

The expected maturity level for the System security engineering capability maturity model (SSE-CMM) used to calculate the level of information security maturity is 5, which is optimized. First, the value difference for each clause is calculated, and this is the maturity level distance. The total value of the overall difference is calculated by adding all values and dividing them by the number

of control objectives. The magnitude of the difference between actual security working conditions and expected security conditions is 2.55, with a 51.1 % disparity in overall information security maturity. Table 4.14 depicts the disparity between actual and planned levels of information security maturity.

There is certainly a substantial gap in maturity level. The parts that follow discuss the importance ratio to the current maturity level as well as the value of the anticipated maturity level. The maturity level for information organization is 2.47, with a gap of 2.53; the human resource score is 2.45, with a gap of 2.55; the assessment of maturity score for asset management is 2.34, with a gap of 2.66; and the evaluation of information security policy is 2.41, with a gap of 2.59. Access Control has a maturity score of 2.57, and the difference is 2.43. The difference is 2.81 and the competency level for cryptography is 2.19. The confidence rating for physical and environmental protection is 2.73, with a difference of 2.27, and the maturity score for operational security is 2.48, with a maturity gap of 2.52, communication security is 2.37, with a gap of 2.63, and system acquisition, development, and maintenance is 2.37, with a gap of 2.63 and maintenance maturity level of 2.45 with a gap of 2.55, supplier Relationships control objectives maturity level of 2.57 with a gap of 2.43, Compliance maturity level of 2.59 with a gap of 2.41, Information security incident management maturity level of 2.32 with a gap of 2.68, and finally Information security aspects of business continuity management maturity level of 2.29 with a gap of 2.71.

Table 4.15. The gap between the current and expected level of information security maturity

No	Information security controls	Maturity		Gap	Gap in %
		Current	Expected		
1	Organization of information security	2.47	5	2.53	50.6
2	Human resource security	2.45	5	2.55	51
3	Asset management	2.34	5	2.66	53.2
4	Information security Policy	2.41	5	2.59	51.8
5	Access Control	2.57	5	2.43	48.6
6	Cryptography	2.19	5	2.81	56.2
7	Physical and environmental security	2.73	5	2.27	45.4

8	Operational security	2.48	5	2.52	50.4
9	Communication security	2.37	5	2.63	52.6
10	System acquisition, development and maintenance	2.45	5	2.55	51
11	Supplier Relationships	2.57	5	2.43	48.6
12	Compliance	2.59	5	2.41	48.2
13	Information security incident management	2.32	5	2.68	53.6
14	Information security aspects of business continuity management	2.29	5	2.71	54.2
Average				2.55	51.1

Figure 4.3 illustrates the overall maturity level of information security in the private banking industry on a radar graph. As shown in Figure 4.3, only three control objectives at level 3 (defined) have been met: A.9 Access Control, A.11 Physical and environmental protection, and A.15 Supplier Relationships. While the vast majority of security control areas are at level 2, (Repeatable but Intuitive). In general, the private banking industry has not achieved level 4 (Managed) or level

5 qualification (Optimized). Any of the security control objectives can be identified.

Figure 4.4. The gap between the existing and expected level of maturity

4.3 Document Analysis

In terms of document analysis, the sampled private banking does have their own information security policy and protocol in place to protect the company from both external and internal threats. As previously addressed in the quantitative data analysis and presentation sections. Only two of the four sampled private banks have agreed to share their information security guidelines, and the researcher attempts to investigate whether the security guidelines are prepared in accordance with the international security standard, which encompasses all assets on the organization's premises. This method of record analysis assists researchers in cross-checking the validity and reliability of questionnaire responses. The following is a summary of the results for various security control areas:

Access control policy and identity management

This approach applies to all of the institution's current facilities and services. The policy amendment and revision guidelines are as follows: “Unless there is special enforcement to update the information protection and access policy in the meantime, it should be updated every three years, subject to prior approval of the Board of Directors,” the researcher deduces from this declaration that there is a significant gap to revise and review the information security policy.

Security Incident Management

Information systems that are suspected to be compromised will be disconnected from the Bank network before the incident has been reviewed, resolved, and the risk has been minimized sufficiently. All information security incidents will be reported for later study and evaluation in order to identify areas where policies, processes, and information security measures can be improved. If the incident is not adequately resolved, the issue should be escalated to the Chief Information Officer.

Physical and Environmental security

Classified information and IT infrastructure, such as the Data Center, Disaster Recovery Center, server rooms, head office organs switches, and all word stations connected to Bank X networks, must be physically secured to reduce business and organizational impacts. For DMZ (Demilitarized Zone) system, device, and network management, equipment and software within the scope of this policy must be administered by support groups authorized by the IT security team. For data security, the data has been divided into four classes.

1. High Risk: information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. i.e., customer account information, payroll, personnel and financial information.
2. Confidential: Data that should be protected to prevent unauthorized disclosure. The user access to such data is limited to what he/she needs to do their job and can only be given to staff by role and responsibility.
3. Internal use: this category is for internal business information but if disclosed o external entities, could result in some level of harm or disadvantage for the company, its employees and customers.

4. Public: information that may be freely disseminated without causing any harm to the Bank, its customers or shareholders.

Human Resource Security (During Employment and termination)

It shall be ensured that employees, contractors and third-party users are aware should aware of information security threats and concerns. In the course of their usual employment, their obligations and responsibilities are built to handle organizational security policy. To reduce potential security threats, all employees, contractors, and third-party users should get enough safety measures, awareness, and orientation in security processes and the proper use of information processing facilities. Management in each division should also ensure that personnel under their supervision are appropriately trained on their information security duties and duties before being provided access to sensitive data or information systems.

Employees, contractors and third-party users who do shall exit the Bank X in an orderly manner. All equipment's and access right associated to their user role should have to be returned and revoked. And whenever an employee change's role with in the Bank the user access right also should have to be reviewed. The review includes cancelling access rights that are no longer needed unless it has been explicitly authorized by the information system owner or authorized delegates.

Compliance

Management must ensure that security policies in their areas of responsibility are implemented and that regular checks are conducted to ensure compliance with security policy and standards. The following individuals adopt and adhere to the organization's security policies and procedures:

- Conducting periodic self-assessments;
- Ensure regular information security awareness updates and
- Initiating assessments, reviews or audits to assess compliance to the information security policy.

Critical information systems should be reviewed at least every two years and the IT auditors shall perform compliance reviews or audit of the implementation of recommendations from information incident reports, when necessary.

The researcher recognizes from the document analysis review that the data collected through the questionnaire are included in the institution's information security policy, which has the foregoing. However, there is a void when the strategy is implemented on the ground. Despite the fact that these information security regulations exist, their content is limited in contrast to industry standards, in this case ISO 27001, and they are either not communicated or workers lack sufficient awareness. This has shown that the organization has not revised its security policy in the last two or three years since higher management has waited for managers to submit proposals on revising the security policy.

4.4 Discussion

This study was carried out to reduce and gradually resolve information security-related difficulties and disasters that arise in a variety of ways by evaluating the existing information security maturity level and identifying security gaps for the Ethiopian private banking industry. Although banking is a key financial organization in the economic sector, it is formally vulnerable to fraud and attack both internally and externally.

The total number of private banks in Ethiopia is 16, according to data acquired from the National Bank of Ethiopia, and the researcher divided them into four groups based on their high profit achievement in the 2019/2020 fiscal economic year. Theoretically, the banks with the highest economic achievement are more vulnerable to security attacks, whereas those with the lowest economic achievement are less important to attackers. Hackers can gain a little amount of money by compromising the lowest bank. As a result, when the bank makes a large profit, it becomes a more attractive target for attackers. As a result, Bank A, Bank B, Bank C, and Bank D have arranged in order of highest to lowest profit attainment, from A to D.

The information security maturity level is not a one-time task; institutions founded on information systems must evaluate their security maturity level on a regular basis, as several researchers suggest. Essentially, when this research began, it aimed to answer two research questions, which are discussed below:

First research question:

"Where is the information systems security maturity level of Ethiopian private banking industry?"

The assessment of information security maturity levels helps in determining the organizations' relevant security processes that must be enforced in order to achieve information and information security system. Maturity level values scale from zero to five are used to measure the level of maturity in line with the Maturity Level Performance Objectives. The information security maturity level was calculated using the System Security Engineering Capability Maturity Model (SSE CMM), which has been detailed in earlier chapters.

According to the study results obtained, the average value of the information security maturity level on the Ethiopian private banking industry in terms of the selected banks is 2.45, and the maximum result on information security maturity level is five (Optimized). This level of significance suggests that information security maturity is at the second level, and that is repeatable but intuitive. And, according to the SSE-CMM assessment criteria, level two means that information security controls exist and are carried out in an ordered and controlled way, but in an unstructured manner.

The value of the difference between the actual information security maturity level and expected information security requirements is 2.55. There is a legitimately significant disparity in terms of value in relation to current maturity level as the expected maturity level's worth. There is an action cycle that is repeated when doing duties connected to information security governance management, but its presence has not been explicitly proven or properly defined, and formal inconsistency exists. As stated in the prior section, private banks must be more secure and knowledgeable on the subject because they handle financial information and must address security.

This research is aimed to assess Ethiopia's private banking industry's current level of information security maturity.

According to (Beshah, 2017), the Ethiopian banking industry's maturity level of information security management is lower than predicted, with weak information security control and management. According to the study, there is also no information security system or standard used by banks as well as no legislative framework enforced by the banking regulatory body. According to the report, the majority of the banks surveyed lack a structured information security standard, 83.3 % lack an information security management standard, and 16.7 % have implemented COBIT, ISO, and PCI DSS independently.

The analysis did not calculate maturity and did not define it with a number, and it was carried out using the DNB (Nederlandsche Bank) maturity level evaluation system. Finally, based on the research findings, the researcher suggests that the maturity level gap be filled by performing an assessment of information security maturity level on a regular basis. Furthermore, banks should offer security awareness training to employees as well as enforce security policies and procedures.

This research has differed by the previous one by majority of the respondents (more than 70%) agreed that their bank has adopted an information security policy, even though there are no institutional framework criteria imposed by regulatory body NBE (National Bank of Ethiopia). The information security division has been identified as a department and employee security staff, which were not previously applicable. There is a noticeable difference between the two studies. However, the information security maturity level must be assessed on a regular basis in order to compare the research results and close the gap.

Although not in financial sector, a related local research was conducted to assess the maturity level of Ethiopian public universities (Ejerssa, 2018). The ISO27001:2013 information security control priorities were used by the researcher, and the study was carried out using the SSE-CMM maturity model evaluation criteria. According to the findings of the study, the majority of the security domain has a maturity level of 2. (Repeatable but intuitive). Another study conducted by (Gera, 2019) on assessing the information security maturity level of hospitals in Addis Ababa using the ISO27002 shows the outcome of maturity level two based on the SSE-CMM maturity assessment model.

The sensitive nature of the data handled by financial institutions distinguishes them from hospitals and educational institutions.

Based on these findings, the researcher concludes that the financial sector's maturity level is nearly identical to that of other sectors. In recent years, the banking industry has seen an increase in the implementation of electronic e-banking services, and the market is now focused on providing superior customer service. In order to provide high-quality service, banks must safeguard the confidentiality, integrity, and availability of their information systems. Financial services have become one of the most common targets for electronic criminals as technology has advanced. Despite this, the study assessed the current level of information security maturity in the private

banking industry and recommended that an acceptable information security management standard and a well-organized information security division be created to fill the gap.

Second research question:

"How can the security gaps be improved to enhance the information security maturity of the private banks?"

The maturity levels are assessed in order to decide the necessary security changes that a company can implement in order to create a better information and information security framework. Using the results of the questionnaire data, the average value of information security maturity level in Ethiopian private banks was measured. The four sampled banks' average maturity level is 2.45, which is level two, and the estimated maturity level is five. Knowing an organization's information security maturity level gives you more trust that its data assets are adequately protected against persistent attacks. It also provides a standardized and systematic mechanism for identifying and assessing information security threats, designing and enforcing appropriate controls, and monitoring and improving the effectiveness of the major security areas specified in ISO 27001 information security control criteria.

Several international standards have also emphasized the importance of an organization's information security strategy. According to ITIL, ISO, and SAN, information security standards should be implemented within the organization, and employees should be familiar with the policy. Bank x has put in place an information security policy, but it does not seem to be well applied across the whole branches. Some employees are unsure of what they are and are not supposed to do. According to quantitative statistics, 30% of employees are unaware that their company has an information security standard.

When analysing the information security guidelines, one of the best practices found was that Bank X was designed magnitude and damage they cause have been classified in the data. As a result, the data has been divided into four categories: high risk, sensitive, internal use, and public. This type of data categorization assists the organization in managing and focusing attention on critically important information. Classified information, such as incident identification based on severity and harm caused, is important for risk-based management (Hove, 2013).

According to the study results, the banking industry is facing both internal and external information security threats. 40.7 % of respondents reported internal attacks, 22% reported external attacks, and 37.3 percent say all types of attacks. To defend against such attacks, private bank top management must understand the value of information security and pay careful attention to information security maturity on a regular basis. They must focus on creating and coordinating Information Security teams, as well as allocating an appropriate budget to meet the department's technological requirements. Furthermore, any employee should follow the information security management system protocol and lock his or her computer whenever he or she leaves the workplace, during lunch or break time, or even when he or she goes to another office, and there should be a policy in place to protect his or her data from desktop change, including the use of strong passwords and frequent changes, which must be implemented by policy.

According to the study's findings, critical infrastructures such as financial institutions, internet service providers, and national security institutions face challenges such as a lack of in-house expertise, difficulty identifying the correct security warning sign, a lack of enabling technologies, and violation of existing security controls. For information security, expertise or trained professionals are required. According to recent studies, technologies do not work independently. Technological solutions make use of people, procedures, and job practices. Trained professionals should use information security software as part of a larger security activity.

4.5 Summary

This section analyses, discusses, and presents the information gathered from study participants. The collected data was interpreted and analysed using the ISO/IEC 27001 information security standard, which is accepted in more than 142 countries worldwide. Since this standard lacks its own metrics for measuring information security maturity, the researcher used SSE-CMM. As a result, the shortcomings and challenges of the private banking industry's information security maturity level have been recognized. The data was gathered using quantitative approaches, and it was also analysed and checked by the Bank's ICT management and experts. According to the research findings, the private banking industry has an overall maturity level of two. The maturity level was 3 for four control objectives out of 14 information security measuring parameters, with

the remaining ten falling into the level 2 category. The subsequent chapter will provide a summary of the research's main findings, conclusions, recommendations, limitations, and future works.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter concludes the whole research. It reviews key findings of the research, conclusions, and recommendations. Finally, suggestions are made for future research to assist other researchers to further explore or expand the current study.

5.2 Summary of Key Findings

This study was carried out to determine the maturity level of information system security in the Ethiopian private banking sector, using data gathered through questionnaires. Through the investigation conducted in sampled private banks, the study intends to identify important information security areas that are more sensitive to security threats and to improve the security competence of private banks.

The information security areas like: Access control, physical and environmental protection, supplier relationships, and compliance are all information security measures that are rated at the highest maturity level, which is level 3 of maturity (Define) procedure. This study also intended to assess the lowest maturity level rated security control objectives, which were discovered to be very weak: cryptography, information security incident management, and information security aspects of business continuity management. These security control areas, however, need improvement. It is possible to ensure the security of information system resources by organizing the best of data security control and employees who are formally recognized willing to commit to handling IS security matters, as well as constructing an organizational framework for ensuring the progress as well as activity of information systems and accountabilities.

The overall availability of information security policy score was 70.3 %. According to the respondents, all policies and procedures are adopted and applied. Almost all employees are expected to sign a confidentiality agreement, and the information security policy must be reviewed on a regular basis, especially by MIS managers.

The challenges of information system security maturity planning identified in these studies in private banks are as follows:

- The information security manual lacks standardized risk analysis and security guidelines.
- There are no mechanisms for tracking information security maturity.
- There is a scarcity of professional and qualified information security specialists.
- Disaster recovery is not well planned for server environments that are located in the same area.
- Inadequate updating and review of information system security guidelines on a regular basis.
- The information security strategy and the IT governance system are not separated or demarcated.
- On a financial system governor, there is a lack of industry guidelines or best practices.
- Lack of information system security requirement awareness among employees.
- Information the gap among departments as well as the enhancement of new emerging threats.
- Insufficient budget allocation and manpower.

5.3 Conclusion

The goal of this study was to measure the current level of information system security maturity in private banks in Addis Ababa, Ethiopia, and to review the maturity results to make recommendations for potential improvements. Attempts were made in this analysis to review and compare the available international standards and guidelines to use them compared to current practice. To evaluate the information system security maturity management at the sampled four private banks. Thus, quantitative data collection and analysis has used.

According to the Systems Security Engineering Capability Maturity Model (SSE-CMM), which is an extensive systematic review system to evaluate the framework that has already been fulfilled and the maturity they have acquired, the outcome of the security questionnaire analysis managed to obtain an estimated return of 2.4 for all of the ISO 27001 controls.

The study determined the degree to which current requirements and guidelines are used in the security maturity management process of private banks' information systems. We discovered that banks do not have a predefined and distinct information protection disaster recovery strategy or risk reduction techniques. However, they are in several ways consistent with international requirements and guidelines such as ITIL, COBIT, and ISO. Some processes, such as data classification and incident escalation to the chief information officer, seem to be well executed. Some processes and practices do not seem to be well-established like, teamwork, risk assessment processes, awareness and training programs, operational risk prevention systems, and post-incident practices such as sharing of experience are examples of factors that limit maturity.

Human resources, especially technical workers, are not well-versed in technological innovations. This increases the company's exposure to information system security threats. According to the findings, the institution performs almost no risk assessment. Failure to conduct regular risk analysis and maturity level measurements exposes IT systems to various attacks caused by emerging technology and incidents. Software suppliers and device providers in the banking industry are not adequately tested for possible risks. Any risks associated with the company's financial services must also be reduced. As per the survey results, private banks do not have their systems evaluated by third parties that have the appropriate resources and experience for risk assessment. It does not perform comprehensive risk assessments on its own. As a result, the organization would be unable to recognize risks regarding financial activities.

5.4 Limitation of the Study

One of the shortcomings is that the study was considering limited sample banks due to time constraints, limited resources, and the sensitivity of the research area. Since the study's focus was information security which deals with enterprise sensitive information most of the banks are not willing to participate on this research. The respondents consciously or unconsciously desire to make their bank and themselves appear good on the outside can result in a bias. Furthermore, banks are unable to share the documents due to concerns about confidentiality. As information systems security researchers, we should respect such concerns when it comes to exchanging sensitive records, even if it limits data triangulation.

Despite the researcher's desire to interview more business and IT personnel from each category, the sensitivity of the research topic, as well as time and resource limitations. Larger sample size would almost certainly, improve the research's accuracy.

Last but not the least, due to the coronavirus (COVID-19) pandemic there were significant issues when we submitted and attempted to communicate to perform the study by submitting a recommendation letter. Participants often do not want to be interviewed.

5.5 Recommendations

Getting systems in place to avoid and detect as many breaches as possible might be a good starting point for securing the information that an institution holds. Today's threat environment generally requires a gradual expansion of information security strategy to identify and respond to threats, as well as the expertise to implement it. The researcher makes the following recommendations based on predetermined current processes and challenges of information security maturity level at private sector banks, so that bank X and other related institutions can use it to manage information security maturity level development more effectively.

According to the survey results, the majority of private banks have their own information security policies that are developed and recorded as guidelines for security procedures. In some institutes, policies and procedures have not been documented, and even security-related work is done carelessly and without any regular form. The user access rules and rights for each specific user should be expressly stated in a policy guideline. In the event of a transition or promotion, each employee's access privileges must be changed.

Human resource security is yet another security regulation that could also be improved. Concerns about human capital protection should be addressed during the hiring process, in agreements, and on the job. Rules governing information security requirements should also be included in the contract of employment. When an employee, contractor, or third-party leaves the institute, he or she must return all of the institution's assets that were used for work under the terms of the contract. Hence, improving human resource security will assist institutes in ensuring that workers are physically and mentally prepared for work and understand their duties and that any improvements in job conditions will not have an impact on information security.

According to the findings of this study, information security incident management in private banking is inadequate. Which obtained a 2.3 in average information systems security maturity protection level and was classified as level 2 (repeatable but intuitive). To avoid asset loss and disruption of institute operations, information systems should be monitored and physically well secured.

As a result of this, the researcher concludes that forming an information security management team is insufficient to ensure security safety and the growth of security maturity. There must be a well-organized and skilled incident management response team, and this team must practice daily to obtain experience. Focus solely on difficult areas such as response time, user report process, and knowledge gap. All IT staff managers, Incident management team members, and other company employees with essential positions must participate in the emergency preparedness practice.

To protect information system and computers from fraud, and unauthorized access, effective procedures should be developed. By incorporating an information security incident response management team into a banking sector organizational structure, the expansion and well-application of information security controls generate the fundamental foundation for information security implementation and management.

Cryptography is another field of information security control that needs enhancement. According to the survey review, it receives a score of 2.19. which is the least of the fourteen control objectives. The controls in this section are intended to serve as a foundation for the proper application of cryptographic solutions to ensure the confidentiality, integrity, and reliability of the information. Despite the fact that institutes introduced encryption through the use of security devices, regulating through the use of appropriate regulations is also important.

According to the ISO27001:2013 standard, cryptography is the method of translating the ordinary plain text into unreadable data and vice versa. It is a way of hiding and transferring data in a specific medium such that only those who are intended to read and process it can do so. Cryptography not only prevents data from manipulation or modification but can also be used for user identification, promoting encrypted messaging methods in which only the sender and intended recipient of communication can show its meaning. As a result, the researcher advises private banks to use cryptography techniques.

Security program planning and integration, something that of security programs, and security governance processes all have an effect on information systems security program management. It is outlined here that security governance mechanisms are a critical variable required for business enablement as well as the operation of security programs within the enterprise. Employee security consciousness can be instilled by joint teams and operations between the company and IT security section, appointed member toward risk awareness and security-aware decision making, and performing frequent corporate social responsibility performance evaluations to determine if they are comfortable with the security goals met by the security teams and leadership. Ensure that the client satisfaction surveys have also been found to be a major influencer of security leadership. Activity concerning is also influenced by information security management and considered more secure.

According to the research findings, there is no strong distinction between the IT service management framework and the information systems security framework. COBIT is a common technology platform that aims to assist organizations in developing, implementing, monitoring, and improving IT governance and knowledge management. The most recent edition, published in 2014, put a greater emphasis on information governance and its role in business performance and enterprise risk management. ITIL, on the other hand, is a framework of international standards for providing IT services. ITIL's systemic approach to IT service management will support organizations in managing risk, strengthening customer relationships, establishing cost-effective practices, and establishing a stable IT community that enables expansion, growth, and transformation.

ISO 27001:2013 is a globally recognized specification for an Information Security Management System (ISMS) and one of the most widely used guidelines. The most recent edition of the standard is ISO/IEC 27001:2013, which incorporates improvements made in 2017. As a result, the implementation of the ISMS should be considered as a separate project. It is important to develop an ISO 27001 implementation structure that includes the identification of tasks, roles and responsibilities, and objectives. This international standard specifies the requirements for creating, enforcing, sustaining, and vital to its success an information security management system in the organization's best interests. It also includes guidelines for identifying and treating information

security threats that are tailored to the needs of the enterprise. The ISO/IEC 27001:2013 standards are designed to be universal and applicable to all enterprises, regardless of form, structure, or type.

We recommend that Bank X execute the following system security standards specified for each level to have regular improvement and monitoring, based on the current identified practice and problems of information security threat, which keeps the maturity level of information system security low:

Banks should undertake the following to reach **level 3** from their current maturity level of 2:

- Banks should be required to create a security standard methodology and follow it.
- When both internal and external security-related incidents are noticed and tracked, coordinate practices to resolve the issue.
- Organize security awareness, education, and training programs.
- Control and manage security services and mechanisms.
- Changes in the operational security posture should be tracked and dealt with in accordance with security goals.
- Implement, monitor, and update information security standards on a regular basis.

Banks should do the following to reach **level 4** from their current maturity level of 3:

- They should be required to set measurable information security targets.
- Manage threat protection performance objectively.
- The job activities and processes clearly show that the customer's security requirements were met.
- Implement proper physical security controls to guarantee that all facilities housing key systems / equipment, as well as physical areas where sensitive data is processed and kept, are safeguarded, and the access to all computer rooms must be carefully restricted.

Banks should undertake the following to reach **level 5** from their current maturity level of 4:

- Increasing organizational capability in terms of process efficiency
- Gather, synthesize, and monitor vulnerabilities and their attributes using a threat risk analysis method.

- To the extent essential to accomplish their roles, all members of the project team are aware of and involved with security engineering efforts.
- Implement and administer a centralized system for detecting, removing, and protecting against harmful code in all forms.
- Banks should focus their improvement efforts on the required commitment at all levels in order to achieve all incremental maturity levels.

5.6 Future Works

To have regular information systems security maturity enhancement and to have a capability to protect the institution's information system from technological advancement threat, we believe conducting more detailed researches will have benefit for financial institutions especially for banks. This research would be used as a guideline for future studies. The following are the researcher's recommendations for future work:

- This research considered limited private banks; if future studies can be done in all of the private banks, the results of this study can be reinforced which may provide additional insights.
- Assessing the security maturity level of an information system is not a one-time job. As a result, evaluating maturity level over time and comparing the results, research how to integrate information security center in banking sectors.
- Construct a framework that allows the financial sector to self-assess their information system security maturity level.
- Academic institutions' prospects and obstacles in reducing the scarcity of highly trained information security professionals.

References

Abbas Toloie Eshlaghy, A. P. (2010). Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity.

Abebe, G. (2020). *A FRAMEWORK FOR HUMAN FACTORS INFLUENCE ON INFORMATION SYSTEMS SECURITY AT COMMERCIAL BANKS IN ETHIOPIA.*

Akhtar, I. (2016). Research Design :- publication at: https://www.researchgate.net/publication/308915548.

Amare, B. (2015). *Assessment of Insider Threat in Ethiopian Banking Industry.*

Arcot Desai Narasimhalu, D. N. (2014). Strategic Assessment of Information Security Maturity: author profiles for this publication at: https://www.researchgate.net/publication/49250590.

Barki, J. S. (2010). User participation in information systems security risk management, MIS Quarterly, vol. 34, no. 3, pp. 503-522.

Beshah, E. B. (2017). *An Investigation on the Current Information System Security Maturity Level of the Banking Industry in Ethiopia.*

Binti, O. J. (2013). Enhancing the Conventional Information Security Management Maturity Model (ISM3) in Resolving Human Factors in Organization Information Sharing. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 11, No. 8, August 2013.

Blank, R. M. (2020). Security and Privacy Controls for Federal Information Systems and Organizations. In *NIST Special Publication 800-53 Revision 4.*

Bogale, M. (2018). *PROPOSING INFORMATION SECURITY AWARENESS PROGRAM FOR ENAT BANK IN ETHIOPIA.*

Borbinha, D. P. (2016). Maturity Models for Information Systems - A State of the Art : Procedia Computer Science 100 (2016) 1042 – 1049.

Bowrin, H. X. (2020). INFORMATION SECURITY IN THE CARIBBEAN BANKS .

BSI-Standard100. (2008). BSI- standard 100 Information Security Management System(ISMS).

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

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Sage Publications.

Deferew, B. (2020). *CYBER HYGIENE PRACTICES AMONGST EMPLOYEES OF ETHIOPIAN COMMERCIAL BANKS.*

deSouza, F. (2010). An information security blueprint, part 1. CSO Online.

Education, I. C. (2019, May 22). Retrieved from ibm.com: https://www.ibm.com/cloud/learn/it-infrastructure-library#:~:text=ITIL%20stands%20for%20Information%20Technology,and%20printed%20them%20for%20distribution.

Ejerssa, N. (2018). *ASSESSMENT OF INFORMATION SECURITY MATURITY LEVEL ON ETHIOPIAN PUBLIC UNIVERSITIES.*

Ferraiolo, K. (1998). The Systems Security Engineering Capability Maturity Model.

Ferrarini, E. M. (2001). The five-access point security plan. Online http://www.enterprisenetworkingplanet.com/netsecur/article.php/752421, pages 1 – 4, accessed 3/20/2005.

Frunhlinger, J. (2020, Feb 10). *The CIA triad: Definition, components and examples. From:*. Retrieved from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.

GEBREHIWOT, Y. (2018). *ASSESSING INFORMATION SECURITY MANAGEMENT USING AN ISO 27001:2013 FRAMEWORK: A CASE STUDY AT ETHIO TELECOM.*

Geoffrey Karokola, S. K. (2011). Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View.

Georg, D. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management Journal of Information Security, Vol. 4 No. 2, 2013, pp. 92-100. doi: 10.4236/jis.2013.42011.

Gera, E. (2019). *ASSESSMENT OF MATURITY LEVEL OF INFORMATION SECURITY MANAGEMENT USING ISO 27002 AT HOSPITALS IN ADDIS ABABA, ETHIOPIA.*

González, K. E. (2019). A variety of information security threats.

Hailu, H. (2015). *THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA – MAY 2015 THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA.*

Hentea, H. N. (2008). Information Security Management Practices.

Hernandez, C. L. (2019). ITIL SERVICE DESIGN :- author profiles for this publication at: https://www.researchgate.net/publication/332116742.

Hove.C., T. M. (2013). Information Security Incident Management: An Empirical Research.

Huntinski, S. G. (2007). INFORMATION SYSTEM SECURITY THREATS CLASSIFICATIONS: Journal of information and organizational sciences, Volume 31, Number 1 .

Irny, S.I. and Rose, A.A. . (2005). *Designing a Strategic Information Systems Planning Methodology for Malaysian Institutes of Higher Learning (isp- ipta), Issues in Information System, Volume VI, No. 1.*

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.*

ISO/IEC27001. (2005). BS ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements. https://doi.org/10.1109/IEEESTD.2005.339589.

ISO/IEC27002. (2013). ISO/IEC27002:2013 Information technology- Security techniques - Code of practice for information security controls.

itSMF-NL. (2006). Frameworks for IT Management : Van Heren Publishing, Zaltbommel, www.vanharen.net .

Karen, S. L. (2010). Compare and Contrast Inductive and Deductive Research.

Kebede, A. (2019). *DESIGNING a FRAMEWORK for SELECTING EFFECTIVE INFORMATION SECURITY AWARENESS DELIVERY METHOD.*

Kevin Christianto, J. L. (2020). IT Strategy Driven Performance Measurement Based on BSC and COBIT.

Khan, S. W. (2015). Cyber Security Issues and Challenges in E-Commerce.

Ladan, S. Y. (2006). Combination of Information Security Standards to Cover National Requirements. World Academy of Science and Technology. .

Lawrence A. Gordon, M. P. (2004). *CSI/FBI Computer Crime and Security Survey.*

Lawrence A. Gordon, M. P. (2006). *CSI/FBI COMPUTER CRIME AND SECURITY SURVEY.*

LLC, P. I. (2017). COST OF CYBER CRIME STUDY :-INSIGHTS ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE.

Luis Enrique Sánchez Crespo, M. P. (2006). Developing a Maturity Model for Information System Security Management within Small and Medium Size Enterprises. https://www.researchgate.net/publication/221399700.

Malik F. Saleh, M. A. (2012). Compliance to the Information Security Maturity Model in Saudi Arabia JOURNAL OF COMPUTER SCIENCE AND ENGINEERING, VOLUME 14, ISSUE 2 .

Marco Spruit, M. R. (2014). ISFAM: The information security focus area maturity model author profiles for this publication at: https://www.researchgate.net/publication/288134391.

Maşlakçı, L. S. (2020). Validity and Reliability in Quantitative Research author profiles for this publication at: https://www.researchgate.net/publication/344379869.

Matin, L. K. (2018). Data Center Risks Analysis Through The COBIT Framework 4.1 author profiles for this publication at: https://www.researchgate.net/publication/330925998.

McCombes, S. (2019). Descriptive research design methods and techniques.

Mohapatra, H. (2018). DATA COLLECTION AND SAMPLING.

Moller, B. L. (2017). Defining Information Security: Received: 15 September 2017 / Accepted: 19 October 2017 / Published online: 15 November 2017.

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

Negash, T. Y. (2019). Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis Completed Research Paper.

Negussie, A. (2015). *PRACTICES, CHALLENGES AND PROSPECTS OF INFORMATION SECURITY POLICY IN ETHIOPIAN BANKING INDUSTRY.*

Ngwum, N. I. (2016). *Information Security Maturity Model (ISMM): A dissertation submitted to The University of Manchester for the degree of Master of Science.*

Ochiche, B. W. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa – Kenya.

Olijnyk, N. V. (2015). A quantive examination of the intellectual profile and evolution of information security from 1965 to 2015. Scientometrics, 105:883-904.

Osamah M.M. Al-Matari, I. M. (2020). Adopting security maturity model to the organizations' capability model, Egyptian Informatics Journal, https://doi.org/10.1016/j.eij.2020.08.001.

Partow-Navid, L. S. (2012). Students Information Security Practices and Awareness. Journal of Information Privacy and Security. https://doi.org/10.1080/15536548.2012.10845664.

Patil, Y. P. (2019). INFORMATION SECURITY author profiles for this publication at: https://www.researchgate.net/publication/330778559.

Pauline Bowen, J. H. (2006). Information Security Handbook: A Guide for Managers, Recommendations of the NationalInstitute of Standards and Technology, NIST SP 800-100.

Perrin, C. (2008, June 30). *The CIA Triad. Retrieved from:*. Retrieved from https://www.techrepublic.com/blog/it-security/the-cia-triad/

Pijpers, T. (2015). *A framewok for financial institutions to achieve maturity level 4 based on the DNB assessement framework.*

Pillitteri, M. N. (2017). An Introduction to Information Security (NIST Special Publication (SP) 800-12 Rev. 1 (Draft))," National Institute of Standards and Technology.

Prayudi, R. a. (2016). A Maturity Level Framework for Measurement of Information Security Performance :International Journal of Computer Applications (0975 – 8887) Volume 141 – No.8, May 2016.

Rainer, J. R. (1991). Risk analysis for information technology. Journal of Management Information Systems, 8(1),. pages 129 – 147.

Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks :Information Systems Research 26(3):150818112523008.

Redlin, T. G. (2017). Innovations, growth and participation in advanced economies - a review of major concepts and findings. International Economics and Economic Policy14:293–351.

Report, P. I. (2014). *Cost of Cyber Crime Study: United States. 2014.*

Rhodes-Ousley, M. (2013). Information Security: The Complete Reference 2nd edition,. USA: McGraw.

Riadi, E. K. (2018). SECURITY LEVEL ANALYSIS OF ACADEMIC INFORMATION SYSTEMS BASED ON STANDARD ISO 27002: 2013 USING SSE-CMM: International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 1, January 2018.

Ryan, J. (2006). Is Information Security or Information Security Awareness the Greater Challenge to the Global Business Enivronment? publication at: https://www.researchgate.net/publication/332117774.

Sahar Al-Dhahri, M. A.-S. (2017). Information Security Management System International Journal of Computer Applications (0975 – 8887) Volume 158 – No 7, January 2017.

Saleh, M. (2012). Information Security Maturity Model International Journal of Computer Science and Security (IJCSS), 2011. 5(3): p. 21.

Saleh, M. F. (2011). Information Security Maturity Model publication at: https://www.researchgate.net/publication/216462795.

Sarantakos, S. (2005). Social Research 3rd edition. New York: Palgrave Macmillan.

Schneier, B. (2002). Secrets and Lies: digital security in a networked world. Indianapolis, Indiana: Wiley Publishing, Incorporated.

Shih, J. D. (2014). Information Technology and Productivity in Developed and Developing Countries https://doi.org/10.2753/MIS0742-1222300103.

Sri Harsha Somepalli, S. K. (2020). INFORMATION SECURITY MANAGEMENT: Holistica Journal of Business and Public Administration, vol. 11, iss. 2, pp. 1-16.

Supriyatna, A. (2014). Analysis of the academic information system security level by combining Standard BS-7799 with SSE-CMM, Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST), ISSN: 1979-911X,Yogyakarta, .

Tebkew, K. (2016). *Information Security Framework for Banking Industries in Ethiopia.*

Tershukov, D. (2019). Analysis of Modern Information Security Threats: NBI Technologies.

Thebestvpn. (2019). thebestvpn. Retrieved Dec 2020, from thebestvpn website: https://thebestvpn.com/cyber-security-statistics-2019/.

Thomson, M. E. (1998). Information security awareness: educating your users effectively. Information Management & Computer Security, 6(4), pages 167 – 173.

Tiago Catarino, B. F. (2016). INCONSISTENCIES IN INFORMATION SECURITY ROLES author profiles for this publication at: https://www.researchgate.net/publication/304396423.

Toezicht. (2014). *Information on 2014Assessment framework for information security*. Retrieved from https://www.toezicht.dnb.nl/en/binaries/51-230767.pdf.

Toyigbé, P. J. (2015). Measuring Information Security: Understanding And Selecting Appropriate Metrics.

Tredinnick, L. (2016). Information security Business Information Review 2016, Vol. 33(2) 76–80 The Author(s) 2016 Reprints and permission: .

Tuan, H. S. (2011). Information Security Management System Standards: A Comparative Study of the Big Five: author profiles for this publication at: https://www.researchgate.net/publication/228444915.

Vasiliki Diamantopoulou, A. T. (2020). From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls.

WALL, D. S. (2015). The Internet as a Conduit for Criminal Activity: pp. 77-98 in Pattavina, A. (ed) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage.

Waxman, M. C. (2013). Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions Electronic copy available at: https://ssrn.com/abstract=2235838.

Yves Barlette, V. V. (2009). The Adoption of Information Security Management Standards: A Literature Review.

APPENDICES

Appendix A: Letter of Request

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

Addis Ababa University
College of Natural Science
School of Information Science

Date: February 25, 2021
Ref No. SIS/19/2021/13

To Whom It Concern

Subject:- Student Tadele Shimels

Dear Sir /Madam,

Student Tadele Shimels (ID.No GSE/9937/11) is graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a M.Sc. Thesis research under the title "Towards Improving Maturity of Information Systems Security in Private Banks in Ethiopia".

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

With Regards

Tibebe Beshah (PhD)
Head, School of Information Science

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

Appendix B: Questionnaire Survey

Dear Participant,

My name is **Tadele Shimels**, I'm conducting a research study entitled ***"Towards improving maturity of Information systems security in private banks in Ethiopia".*** As partial fulfilment of my MSc degree program. I am respectfully requesting you to join in this study by answering the survey questions enclosed.

The below survey will take between 25 and 30 minutes to finish. This survey is completely confidential and no one, even the researcher, will not be able to link your responses to personal identities. You also might want to communicate with experts at your institution regarding specific questions. ***Your response is extremely important and valuable*** for the success of the research to achieve the objective of the study by indicating possible gaps, if any, and possible solutions that need to be taken by concerned organs.

I appreciate it in advance if you could take a few minutes of your important time to complete all of the questionnaire's inquiries.

Sincerely,

Tadele Shimels.

Mobile Number: +251- 913-324951

Email: metikest21@gmail.com

Instruction: This questionnaire has two parts. For each object, place a √ sign in the curly braces.

Part I: General Information: Respondent's Information

1. Respondent's Information

1.1 Respondent Job Tittle …….

1.2 Qualification:

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

1.3 Years of Experience

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

2. Organizational Information

2.1 Has the organization's information security ever been breached?

Yes [ ] No [ ] Don't Know [ ]

- If yes, is the attack emerges from internal, external or both?

Internal [ ] External [ ] Both [ ]

2.2 Are there any security standard does your organization follow's?

Yes [ ] No [ ] Don't Know [ ]

If your answer is Yes, which one is from the following

ISO [ ] COBIT [ ] ITIL [ ] Other please specify……..

2.3 Are there dedicated personnel employed for information security control and protection?

Yes [ ] No [ ] Don't Know [ ]

If your answer is Yes, did they attend security-related training(s).

Yes [ ] No [ ] Don't Know [ ]

Part II: Management of Information Security in the Current situation.

Please mark (right) in the box that corresponds to your response. Your decision would have the following implications:

0 is None	1 is Initial	2 is Not-Defined	3 is Defined	4 is Managed	5 is Optimized

Range	Descriptions
0 None	The management of the company seems unconcerned about the necessity of information system security.
1 Initial	Without prior planning, the company executes proactive deployment and installation of information security in compatible with the demands of existing situations.
2 Not-Defined	The organization has a structure that is repeated in conducting activities connected to information security governance management, however its presence has not been properly defined, and formal irregularity is still occurring.
3 Defined	The Organization has established and documented policies and procedures that have been disseminated to all levels of management and workers and are expected to be followed and implemented in daily operations.
4 Managed	The organization has a set of signals or quantifiable metrics that act as targets and objective measures of performance for each program.
5 Optimized	The organization has built "industry standard" information security governance.

Nº	Question	Your Choice					
		0	1	2	3	4	5
	Organization of information security						
1	Roles and responsibilities for protecting an individual information asset were clearly defined.						
2	Your institution has a dedicated system security personnel's with clearly defined responsibilities for information security.						
3	Addresses remote working. It's designed to make sure that anyone who works from home follows appropriate practices and use secured private network.						
	Human resource security	**0**	**1**	**2**	**3**	**4**	**5**
4	Are security tasks and responsibilities clearly outlined in the contract of employment at your institution?						
5	All institution personnel and third-party users receive adequate information security awareness training as well as frequent updates on organization security practices.						
6	Remove or change their access, when they no longer hold that role either because they've left the organization or changed positions.						
	Asset management	**0**	**1**	**2**	**3**	**4**	**5**
7	All information has classified to ensure the information assets subjected to access for an appropriate level of defence.						
8	There is a secured process for handling and ensures sensitive data is not subjected to unauthorized disclosure, modification, removal, or destruction.						
	Information security Policy	**0**	**1**	**2**	**3**	**4**	**5**
9	An organization information security policy is properly documented, published and available to all employees.						
10	The information security policy considers all stakeholders like employees, departments, branches, vendors and service providers						
11	Security rules and procedures are reviewed and implemented as conditions change.						

12	The security policy has been properly implemented and is successful in ensuring the information security.						
13	Your institution conducts formal risk management analysis activity before developing an information security policy.						
14	Your organization follows a standard or framework while implementing information system security.						
	Access Control	**0**	**1**	**2**	**3**	**4**	**5**
15	Access controls in place to allow the user only ever have access to the limited resource that they have been granted specific permission to utilize.						
16	For authorizing access to the system of information systems and services, there is a user access control policy declaration.						
17	There is a mechanism in place to guarantee that users select and use passwords in accordance with appropriate security practices.						
18	Audit logs and system logs are used to capture security-related occurrences and are retained for a set length of time to aid in future investigations and authentication tracking.						
	Cryptography	**0**	**1**	**2**	**3**	**4**	**5**
19	Has your institution use encryption? (Hiding sensitive information)						
20	Organizations properly and effectively monitor encryption, to protect the confidentiality, integrity, and availability of data.						
	Physical and environmental security	**0**	**1**	**2**	**3**	**4**	**5**
21	Electricity, cabling, and wireless connectivity transporting data or supporting information services are all safeguarded from theft or harm.						
22	Security controls and policy definition and use to protect physical machines that contain sensitive or critical information.						
23	Server rooms, Datacentre, and sensitive areas are protected and supervised regularly, and only authorized users have access to log in.						

24	To prevent the loss, destruction, or theft of an organization's information assets, permission and checking are performed on every equipment entering and departing.						
	Operational security	**0**	**1**	**2**	**3**	**4**	**5**
25	Addresses operational procedures and responsibilities, ensuring that the correct operations are in place to conduct.						
26	Addresses malware, ensuring that the organization has the necessary defences in place to mitigate the risk of infection.						
	Communication security	**0**	**1**	**2**	**3**	**4**	**5**
27	Ensuring that the confidentiality, integrity, and availability of information communication in those networks remain intact.						
28	Security of information has ensured in transit, whether it's going to a different part of the organization, a third party, a customer, or another interested party.						
	System Acquisition, development and maintenance	**0**	**1**	**2**	**3**	**4**	**5**
29	When new systems are launched, modified, or expanded, information system security requirements are identified and addressed.						
30	Protects and controls the security needs for internal systems as well as those that deliver services over corporate networks in a proper manner.						
	Supplier Relationships	**0**	**1**	**2**	**3**	**4**	**5**
31	There is safeguarding of an organization's precious assets that are accessible to or influenced by suppliers or vendors.						
32	Contracts have been designed and executed to ensure that both parties maintain the agreed-upon degree of information security and customer service.						
	Compliance	**0**	**1**	**2**	**3**	**4**	**5**
33	Your institution identifies relevant laws and regulations of information security. Which helps to understand legal and contractual requirements, mitigating the risk of non-compliance and the penalties that come with that.						

34	There is a specific procedure in place to sanction members who violate organizational security standards and procedures.						
35	Does the culture of security compliance design by NBE (National Bank of Ethiopia) Has the organization's attitude toward information security influenced its work methods and service offerings?						
	Information security incident management	**0**	**1**	**2**	**3**	**4**	**5**
36	There is an incident handling and monitoring plan in place that takes into account the classification and severity of information security problems.						
37	Is there a process in place for timely reporting of information security incidents and vulnerabilities, as well as action on disclosed information security events?						
	Information security aspects of Business continuity management	**0**	**1**	**2**	**3**	**4**	**5**
38	Discusses the problem of information security persistence by implementing actions that can be taken to ensure the business continuity plan platform.						
39	There is an efficient system in place to manage potential damage by implementing redundancy and assuring the availability of information assets.						

THANK YOU!

Appendix C: Reference controls, control objectives and clause

Section	Name of Controls	Control Objectives	Number of Clauses
A.5	Information security policies.	To provide management guidance and support for information security in compliance with company needs and applicable laws and regulations.	2
A.6	Organization of Information Security	To build a management framework for initiating and controlling information security implementation process inside the organization.	7
A.7	Human Resource Security	To ensure that workers and suppliers understand their jobs and are qualified for the positions for which they are being evaluated.	6
A.8	Asset Management	Identifying organizational assets and defining appropriate risk mitigation tasks.	10
A.9	Access Control	The policies in this section strive to limit access to information and information assets in accordance with business requirements, using formal processes to grant or remove access privileges. Physical or logical access, as well as access made by individuals and information systems, are all taken into account by the controls.	14
A.10	Cryptography	To ensure that cryptography is used correctly and effectively to safeguard the anonymity, integrity, and/or integrity of the information.	2

A.11	Physical and Environmental Security	The procedures in this section are designed to prevent illegal access to physical places, as well as to safeguard infrastructure and instruments that, if corrupted by natural or human activity, could jeopardize information assets or business activities.	15
A.12	Operational Security	Moreover, measures in this section require the capacity to record events and collect evidence, as well as frequent vulnerability verification and the adoption of safeguards to prevent audit attempts from disrupting performance.	14
A.13	Communications Security	The rules in this area are designed to secure network infrastructure and services, as well as the data that goes through them.	7
A.14	System Acquisition, Development and Maintenance	The procedures in this section are designed to ensure that information security is taken into account throughout the implementation phase.	13
A.15	Supplier Relationships	The measures in this area are designed to guarantee that outsourced activities conducted by suppliers take information security measures into account and are effectively monitored by the business.	5
A.16	Information Security Incident Management	The regulations in this part attempt to establish a framework for ensuring effective communication and control of security incidents, so that they can be resolved in a timely manner and include evidence retention if needed, as well as quality management to minimize occurrence.	7

A.17	Information Security aspects of Business Continuity Management	The policies in this part are designed to ensure the continuity of information security management and the underlying infrastructure systems in the face of adversity.	4
A.18	Compliance	The restrictions in this segment aim to include a structure for preventing legal, legislative, regulatory, and contractual violations, as well as to ensure independent confirmation that information security is implemented and effective in accordance with the ISO 27001 standard's defined policies, procedures, and requirements.	8