ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

DEVELOPING AN INFORMATION SYSTEM SECURITY FRAMEWORK: A CASE STUDY AT MINISTRY OF FINANCE (MOF)

A Thesis Submitted to School of Graduate Studies of Addis Ababa University

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Information Science

By: BINIYAM T/SILASSIE G/MARIAM

Advisor: TEMTIM ASSEFA (PhD)

APRIL, 2024

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

DEVELOPING AN INFORMATION SYSTEM SECURITY FRAMEWORK: A CASE STUDY AT MINISTRY OF FINANCE (MOF)

A Thesis Submitted to School of Graduate Studies of Addis Ababa University

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Information Science

By: BINIYAM T/SILASSIE G/MARIAM

Name and signature of Members of the Examining Board

Temtim Assefa (PhD)	_____	_____
Advisor	Signature	Date
Lemma Lessa (PhD)	_____	_____
Examiner	Signature	Date
Getachew Hailemariam (PhD)	_____	_____
Examiner	Signature	Date

Metadata

Student Name: BINIYAM T/SILASSIE G/MARIAM

Advisor: TEMTIM ASSEFA (PhD)

Department: Information Science

Qualification: Master of Information Science

Study Title: Developing an Information System Security Framework: Case Study at the Ministry of Finance of Ethiopia

Knowledge Area: Information Security

Keywords: Information security, Cybersecurity, framework, digital financial

Type of Research: Applied Research

Research Paradigm: Interpretivism

Research Design: Case study

Status: Final Thesis

Department: School of Information Science

Submission Date: Feb 09 2024

Declaration

I, Biniyam T/silassie G/mariam, declare that the content presented in this thesis for the Master of Information Science Degree, titled:

"**Developing an Information System Security Framework for Ethiopian Ministry of Finance**," is entirely my own original work. I confirm that I have not previously submitted this work, either in its entirety or in part, to any other university or higher education institution for the purpose of obtaining a degree.

I also confirm that I have fully acknowledged all sources of information that I used in my research, adhering to the rules and regulations set out by the university.

Signature: _____

BINIYAM T/SILASSIE G/MARIAM

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

Advisor's Signature: _____

TEMTIM ASSEFA (PhD)

ACKNOWLEDGEMENTS

I would like to express my heartfelt appreciation to the Almighty Creator for priceless love, guidance, blessing, good health, giving hope, wisdom, and the precious gift of life.

I would like to express my deep appreciation to my advisor, Dr. Temtim Assefa, for his priceless guidance, exceptional leadership, and unconditional support throughout this journey of research from start making out research title reformulating research questions, data collection interview questions and evaluation checklist questions. Dr. Temtim, I am truly grateful for your solid determination, trust in my abilities, timely feedback, and patience, which played a crucial role in bringing this study to its successful completion. Your unique approach, advice, commitment and dedication, combining gentle pressure with realism, made a significant difference and effort to come up to the completion of this study. I don't have any words to express my gratitude for being his an exceptional mentor and supporting me.

I would like to extend my gratitude to the Ministry of Finance's management and the entire teams involved for their valuable time and participation in the interviews and framework evaluation. Thank you, ladies and gentlemen, for your significant contribution to my study. Your input has been immeasurably appreciated, and without it, I would not have been able to successfully complete this research.

Finally, I would like to express my sincere gratitude to my close friends, family relatives, and all those who have supported me throughout this study. It is because of your solid support, encouragement, and inspiration that I have become the person I am today.

Thank you all!!!

Abstract

The digital financial institution sector encompasses a wide range of organizations, from small community microfinance institutions to large international corporations. In recent years, the financial sector has experienced a rapid growth in cybersecurity threats, as cyber-attacks targeting financial institutions have become increasingly predominant. These threats put sensitive data and organizational security at risk. Increasing the issue is the absence of a recognized information system security framework that can protect financial data between various customers such as banks, customs, governmental organization up to remote woreda and license registered traders. The study utilized a qualitative approach, specifically a case study and design science research methods. Data was collected through interviews with domain experts and document reviews. Thematic coding was used to analyze the collected data, which identified several key themes necessary for developing the information security framework.

The study revealed that there were different security challenges which include lack of cybersecurity expertise and awareness, various threats, facilitating conditions such as budget allocation and capacity building, preventive mechanisms encompassing technical and non-technical solutions, and security auditing and evaluation, as well as SOC real-time traffic monitoring. The study also developed Information System Security Framework for Ethiopia Ministry of Finance (MoF). The proposed framework serves as a guideline for the Ethiopian Ministry of Finance (MoF) to enhance Cyber resiliency, manage cyber threats and risks, and implement cybersecurity best practices. This proposed framework contributes to the government's held-on long-term digital Ethiopia plan at 2025 and complements existing initiatives aimed at infrastructure development and investment in cybersecurity. Domain experts who are Cyber experts/professionals at MoF review this proposed framework and they confirmed as it is relevance, applicability, usability, and effectiveness in addressing information system security issues within the Ethiopian MoF and other similar organizations.

Keywords: information system security framework, information/Cyber security, digital financial

Contents

LIST OF FIGURES

Abbreviation And Acronyms in This Thesis

Acronym/abbreviation	Descriptions
AAA	Authentication Authorization & Auditing
AD/DC	Active Director/Domain Controller
AV	Antivirus
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPMI	Committee on Payments and Market Infrastructures
DDOS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
DOS	Denial of Service
E-GP	Electronic Government Procurement System
Ethio-CER^{2}T	Ethiopia Computer Emergency Readiness & Response Team
IBEX	Integrated Budget and Expenditure System
ICT	Information & Communication Technology
IDS	Intrusion Detection System
IFMIS	Integrated Financial Management Information System
INSA	Information Network Security Agency
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSP	Information Systems Security Policies

IT	Information Technology
MoF	Ministry of Finance
NAC	Network Access Control
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
SDN	Software-Defined Networking
SOC	Security Operation Center
WAF	Web Application Firewall
ZDNet	Business Technology News Website

CHAPTER ONE

INTRODUCTION

1. Introduction

ICTs have become an integral part of our daily life. The adoption of ICTs has perceived substantial growth, with penetration rates rising from 6% in 2000 to 43% in 2015 in both personal and business contexts. Furthermore, it is projected that there was a yearly increase of 5% in ICT usage (ITU, 2016). This widespread adoption of ICTs has proven to be a critical driver of development, innovation, and economic progress, even in the under developed countries. Now a days, computers have been used in various society, including aerospace, business, education, government, defense systems, banking, healthcare and so on.

ICTs offer substantial advantages, but they also pose inherent risks, primarily due to the ease of unauthorized access to and misuse of data (World Economic Forum, 2020). The World Economic Forum (2020) emphasized that the frequency, complexity, scale, and impact of cyber-attacks have all perceived a rising trend. As our world becomes increasingly interconnected and dependent on digital systems, there is a growing anxiety regarding the vulnerabilities of the Internet, which serves as the backbone for various financial operations, including commerce and the entire financial systems.

Ethiopia has comprised technology as a means to drive service delivery and foster economic development. With the introduction of the West Africa Cable System (WACS) connectivity in May 2012, Ethiopia has seen improved network communications and the provision of reliable Internet services. However, the expansion of Internet usage has also given rise to a new form of crime known as cybercrime (Wall, 2015). During data collection and document reviews, it was observed that the Ministry of Finance (MoF), as the financial sector regulator, lacks an officially recognized cybersecurity framework to safeguard online transactions involving digital financial data exchanged between banks and customers. This absence of a formal cybersecurity framework poses a challenge in ensuring the security and integrity of digital financial transactions. This deficiency can be attributed to a lack of governance, supporting systems, processes, and procedures to effectively mitigate cyber threats associated with online transactions. According to Kaspersky

(2020), financial institutions like banking systems were targeted by approximately over 22 percent of malware attacks.

In the present era, financial institutions have modern advancements in conducting business electronically. In Ethiopia, almost all financial institutions have incorporated electronic banking and mobile banking in various forms. The evolution of technology has become the way for online banking and e-commerce, facilitating financial transactions worth millions of dollars through network connections in the cyberspace. However, this increased dependence on online banking services has also increased the risk of Internet computer fraud in the financial sectors (Bhasin, 2015).

As businesses operate in an increasingly interconnected world and offer more digital products, the risk of successful cyber-attacks for financial institutions also increases. It is not a longer question about the possibility of an attack will happen but rather when it will occur. The invention of the fourth industrial revolution, such as AI, machine learning, robotics, and Internet of Things (IoT) devices, which bring disruptive impacts on technologies, including emerging technology-driven financial services, further amplifies the risk (Rahman & Abedin, 2021). Consequently, with the evolution of technology and the digitalization of financial business processes, safeguarding the financials' asset data has become a crucial driving force for the necessity of protecting online transactions. Therefore, there is an urgent need for the Ethiopian financial sector to take the initiative and adopt an information system security framework to ensure the security of online transactions.

1.1. Statement of the Problem

As Ethiopian financial institutions continue to depend heavily on digital technologies to carry out their operations, they are becoming more vulnerable to cyber threats Currently, according to the Ministry of Finance, there is a lack of a well-established information system security framework for protecting online transactions involving financial data between various customers, such as banks, customs, and licensed registered traders in the financial sector. Girma (2020) developed a comprehensive human factor model for information system security in commercial banks. This study, however, considered only the human factor without considering the technological factors.

Despite investing in advanced security technologies such as firewalls, intrusion detection and prevention systems (IDS/IPS), licensed software, and antivirus, organizations, especially in the

financial sector, the sector is facing an alarming rise in security threats, vulnerabilities, and data breaches in their information systems due to lack of comprehensive tailored information system security framework for organizations (Carmi & Bouhnik, 2021).

Semlambo et al. (2022) conducted a study to investigate the influencing factors related to security. They categorized these factors into four perspectives: human factors, factors of the work environment or organization, ISP policy issues, and individual factors. The human factors encompassed aspects such as a lack of skills and knowledge among employees, negligence in following security protocols, and the level of trust within the organization. Factors of the work environment or organization included management support for security measures, workload pressures, and the overall safety culture within the organization. Information security policy (ISP) issues focused on the adequacy and effectiveness of information security policies, involving factors such as policy-making participants, policy enforcement, and the scope of policies. Lastly, individual factors considered characteristics such as the age, education level which are IT and non-IT related, and work experience of employees. By categorizing these influencing factors, this study provides valuable insights into the various dimensions that contribute to security challenges and threats.

According to the study of Temtim and Alpha (2021), they identified four institutional factors that influence compliance with Information Systems Security Policies (ISSP). Among these factors, top management support (engagement), information security awareness and training, and accountability (responsibility) were found to be the most significant organizational factors shaping employee attitudes and behavior towards compliance with existing ISPs. However, the researchers did not find a positive impact or influence of audit and monitoring on users' compliance behavior to ISSP. This suggests that while certain factors play a crucial role in promoting compliance, the effectiveness of audit and monitoring in ensuring compliance may be limited. The study did not include technological and individual factors that influence users' compliance to ISSP.

Alotaibi and Furnell (2016) conducted a study to identify, examine, and prioritize significant organizational factors that positively influence information security compliance. From their research, they identified five key factors: control security (monitoring), awareness and training, sanctions, rewards, and trust between employees. They emphasized the importance of increasing or developing employee knowledge, skills, and awareness of information security policies to

mitigate information security threats and breaches. Additionally, Nord et al. (2020) found that awareness of information security policies, gender, age, and IT knowledge and skills have a positive relationship with the impact of employee habits on compliance with Information Systems Security Policies (ISSPs). These studies collectively emphasized the importance of organizational factors, employee knowledge and awareness, and individual behaviors in promoting information security compliance.

Hence, the existing studies have primarily examined organizational, technological, social, or individual factors in isolation, which may not provide holistic solutions to the challenges of information system security within organizations. To address this gap, the presented research aims to develop a comprehensive information system security framework that combines organizational, technological, and individual aspects rather than isolation by identifying these critical factors from empirical data on existing information system security prevention practices at the Ministry of Finance (MoF).

The proposed information system security framework can provide guidance and ensure the security of online transactions involving financial data between different customers such as banks (national bank of Ethiopia, commercial bank of Ethiopia), customs, governmental finance organizations including remote woreda-Net and license registered traders.

1.2. Research Questions

The primary research question was how to develop an information system security framework that would provide guidance to the Ethiopian Ministry of Finance (MoF) to effectively safeguarding financial data and technological resources.

However, there are a lot of other established ISS frameworks, such as ISO 27001. This research question is about the organizational context at the Ministry of Finance.

The international one is more complex and cannot be implemented in an Ethiopian context. The proposed framework emerges from the empirical data so that it has better explanatory power for the organization’s security systems. This proposed framework is also a lightweight framework that can be easily implemented by cybersecurity practitioners, cyber security experts, policymakers, etc.

Specific research questions:

i. What are the main information system security threats at Ethiopian MoF financial institution's cyberspace?
ii. What are the implemented information system security prevention mechanisms in the Ministry of Finance context?
iii. How to develop an information system security framework that will serve as a guidance for improving existing information system security practices at Ethiopian MoF?

1.3. Research Objectives

The primary aim of this research was to develop an information system security framework that would provide guidance to Ethiopian Ministry of Finance (MoF) financial institution in protecting online digital financial transactions involving financial data between different customers.

The **specific objectives** of this research are as follows:

i. Examine and analyze the different information security threats at the Ethiopian Ministry of Finance (MoF) financial institution.
ii. Assess the effectiveness and adequacy of the existing information security policies and standards in place
iii. Develop an information system security framework specifically tailored to guide the Ethiopian MoF financial institution in protecting the security of digital financial transactions.

1.4. Significance of the Study

The importance of this study is used for cybersecurity practitioners and framework evaluation as well as used for users' compliance to information security practices. Given the potential for the deployment of various ICT services in Ethiopia, as highlighted in the national digital Ethiopia plan at 2025, it is crucial for all stakeholders to actively contribute and concentrate their efforts to ensure cyber-safety. This research serves as one such initiative, aiming to assist the financial sector in implementing measures that promote cybersecurity and support overall growth in this area.

Moreover, the implementation of an information system security framework in Ethiopia can greatly benefit financial institutions by offering insights into their perspective on information and cybersecurity risk management. The development of such a framework specific to the financial

sector would help rationalize processes and provide guidance on standard requirements. This would make a significant contribution to the understanding of information system security risks and strategies in Ethiopia. Additionally, it would assist financial institutions in determining the appropriate level of rigor for their information system security programs, thereby enhancing their overall security posture.

1.5. Motivation of the Study

In today's digital landscape, the importance of robust information system security cannot be overstated. As organizations increasingly rely on technology to drive their operations and store sensitive data, the need for a comprehensive security framework has become the most important. The motivation behind this research topic is to develop a comprehensive information system security framework that can effectively address the evolving threats and challenges faced by organizations, especially at the Ministry of Finance (MoF).

The rapid advancements in technology and the growing sophistication of cyber threats have made it crucial for organizations to proactively address security concerns. Traditional security measures often fall short in providing the necessary protection, as they fail to keep up with the dynamic nature of the threat landscape. This research aims to address this gap by developing a security framework that is adaptable, scalable, and capable of mitigating a wide range of security risks.

The primary motivation for this study is to develop an Information System Security Framework for the Ethiopian Ministry of Finance (MoF) with a robust and practical tool to enhance their information system security. By developing a comprehensive information system security framework, the research aims to assist organizations in identifying and addressing vulnerabilities, implementing effective security controls, and fostering a culture of security awareness among employees. This proposed framework will serve as a guiding principle for organizations to navigate the complex and ever-changing world of information system security.

1.6. The scope of study

The study specifically concentrated on the development of an information system security framework within the digital financial institution of the Ministry of Finance (MoF). MoF is the focus of this study because it is the financial sector regulator, and the research is examining the lack of an officially recognized information system security framework within MoF to protect

online transactions involving digital financial data between banks and customers. As the central financial authority, the MoF's role and policies in this area are crucial to understanding the cybersecurity challenges in the financial sector. This was achieved through a systematic review of existing cybersecurity frameworks and standards, information security policies, as well as incorporating insights from interviews. It is important to acknowledge that alternative approaches, such as examining cyber-threat indicators, may provide a deeper understanding of essential factors for the framework. Additionally, it is observing that there are various methods for promoting cyber resilience in the financial sector, but the primary focus of this study was on the development of an information system security framework.

1.7. Thesis Outline

The structure or organization of this thesis is organized as follows:

Chapter 1: This chapter provides an introduction to the study, including sections on the problem statement, objectives, research questions, significance of the study, and scope of the research.

Chapter 2: This chapter presents a comprehensive literature review on various information security practices, cybersecurity risks, and existing frameworks and standards in the field of information/cybersecurity.

Chapter 3: This chapter outlines the research methodology employed to achieve the study objectives and address the research questions mentioned in sections 1.2 and 1.3. It includes discussions on the research paradigm/philosophy, research design, research population, sampling techniques, data collection and analysis methods, as well as ethical considerations.

Chapter 4: This chapter analyzes the data collected through semi-structured interviews, evaluates the proposed framework using appropriate techniques, and provides a detailed discussion of the study's results and findings.

Chapter 5: This chapter concludes the study by summarizing the main findings, offering recommendations, highlighting any limitations of the research, and suggestions for future work.

1.8. Chapter Summary

In this chapter, the study's context is established, including the research problem statement, specific research objectives, research questions, significance of the study, motivation of the study, and scope of the study. The chapter also provides an outline of the thesis. The next chapter two focuses on reviewing the existing research literature.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This Chapter reviews research conducted on the overall security landscape, beginning with the operational definition of terms such as information security and the concept of cybersecurity. This serves to establish a solid foundation for addressing the core issues of the study. Additionally, a thorough literature review is conducted to gain a deeper understanding of the nature practices of information security and cybersecurity. Furthermore, an analysis is undertaken to examine various existing cybersecurity frameworks. Finally, a summary of the chapter is provided.

2.2. Information system Security

Information security refers to the practice of protecting information and data from unauthorized access, use, disclosure, disruption, modification, or destruction (Bulgurcu, Cavusoglu & Benbasat, 2010). It involves implementing measures and safeguards to ensure the confidentiality, integrity, and availability of information asset (Bouveret, 2018). Information security aims to prevent unauthorized individuals or entities from gaining access to sensitive data, as well as safeguarding against potential threats, such as cyber-attacks, data breaches, and theft. This includes implementing security controls, such as encryption, access controls, firewalls, and intrusion detection systems, to mitigate risks and maintain the privacy and integrity of information. Additionally, information security involves establishing policies, procedures, and guidelines to govern the proper handling and protection of organization's information assets and information systems.

In today's digital age, cybercrimes pose a significant threat to digital financial institutions throughout the world, resulting in substantial financial losses amounting to billions of dollars (Khan, 2018). With their crucial involvement in providing public financial services to both banking institutions and customers, financial institutions have become prime targets for cyber-attacks (Eloff and von Solms, 2000). This is primarily due to their key role in payment systems, as well as the extensive amount of sensitive customer information they handle. As a result, there is a growing demand to enhance cybersecurity measures by implementing robust governance, security

policies, procedures, processes, and technological solutions to effectively mitigate cyber risks (Crisanto & Prenio, 2017).

According to World Economic Forum (2020), many organizations have implemented remote work policies in response to the COVID-19 pandemic, making digital communication the main method of operation. Unfortunately, this shift has created an opportunity for attackers, as remote work setups often lack the same level of security measures found in traditional corporate environments. Cybercriminals are capitalizing on this situation by leveraging the COVID-19 pandemic as a means to target companies. They use tactics such as sending phishing emails with COVID-19 themes, deceiving individuals into clicking on malicious links that download malware onto their devices such as computer, smart phone, tables etc.

According to a report published by ZDNet in 2020, there has been a significant increase of 238% in cyberattacks against financial institutions, which can be attributed to the COVID-19 pandemic.

The COVID-19 pandemic has had a deep impact on the way people work, leading to significant challenges for businesses worldwide, particularly in the financial sector. From a technological perspective, companies have had to undergo substantial changes to ensure that all necessary tools are in place to facilitate remote work for their entire workforce. The crisis of COVID-19 has obliged financial institutions and other companies to enhance their digital offerings, improve online services, and expand their digital touch with customers. For instance, many banks are encouraging customers to utilize their digital platforms as a means of limiting the spread of the virus through social distancing. However, this increase dependance on digital technologies has also emphasize the risk of cyberattacks, as stated by the World Economic Forum (2020). That is why, the digital transaction volume has been rapidly increasing worldwide following the COVID-19 pandemic, along with a corresponding rise in cyber-attacks.

2.3. The growth of Cybersecurity Threats and Attacks on the Financial Sectors

Technological advancements have brought significant benefits and innovations to various aspects of society, as highlighted by Erastus, Jere, and Shava (2017). These advancements include e-commerce, modernized business processes, enhanced connectivity, easy access to information, and rapid communication. The financial sector has also contained such benefits and innovations, through implementation of mobile banking, credit cards, and Internet banking, as mentioned by Umanailo et al. (2019).

While Information Technology (IT) has undoubtably brought numerous benefits, it also carries certain drawbacks, as pointed out by Erastus et al. (2017). One of the major disadvantages is the risk of information security breaches and the existence of insecure ICT (Information and Communication Technology) environments. The widespread adoption of the Internet has connected countless end-users, including cybercriminals, leading to an increase in illegal activities conducted online. Moreover, the advancements in technology have contributed to the rise of cybercrimes such as credit card theft, hacking of websites, and unauthorized access to Internet banking facilities, as highlighted by Umanailo et al. (2019). It is important to recognize that while technology poses threats, it also offers solutions, as it is a double-edged sword.

The widespread connectivity of end-users to the Internet has made them vulnerable to cybercriminals. With the shift from traditional paper-based transactions to electronic transactions, organizations now rely on cyberspace for information sharing. This includes conducting activities such as Internet banking and e-commerce transactions, which are not boundary by physical limitations (Umanailo et al., 2019). According to The Global Risks Report (2018), cyber-attacks are considered one of the top five global risks in terms of perceived likelihood. Among the various cyber threats, ransomware has emerged as a significant concern for organizations, and this trend is expected to persist in the coming years (Borrion & Yuryna Connolly, 2020).

The digitalization of business processes in the financial industry has made technology as a critical driving force, emphasizing the need for robust cybersecurity measures to protect financial valuable data (Mohammed, 2018). To effectively mitigate cyber threats, the financial industry must establish a cybersecurity framework that aligns with their business processes. This framework necessitates a different security mindset and approaches to areas such as risk management and mitigation. The ultimate goal is to create a strong cybersecurity framework supported by effective laws and regulations that encourage trust and confidence between financial institutions and their customers. Examples of such measures include the Electronic Fund Transfer Act (EFTA) and regulatory bodies like the Federal Trade Commission (FTC) that work towards safeguarding these interests.

To address the evolving cyber risk landscape, financial institutions must take proactive steps to mitigate these risks and enhance their ability to withstand cyber-attacks. This involves implementing various security measures to protect their systems and increase their resilience.

Financial sectors worldwide have recognized the importance of investing in technology, personnel, internal processes, third-party vulnerability management, threat intelligence, and incident response capabilities. Measures such as incident response protocols, training and awareness programs, asset management, third-party cyber risk management, and vulnerability management have been adopted by most financial sectors as part of their comprehensive security strategies (Mohammed, 2018).

Some of the current cybersecurity vulnerabilities or weaknesses in the financial sector include:

- **Mobile and Web Banking security**

The convenience offered by mobile and web banking technologies is undeniable, but it also comes with a downside; they are vulnerable to various types of attacks, with malware attacks being a significant concern (Yildirim, Varol, 2019). In fact, according to a report by ZDNet in 2018, bank web apps were found to be the most vulnerable to hacking attempts.

- **The use of third parties**

The Dependance on third-party services introduces security risks to the protection of data. The financial systems are vulnerable due to their dependence on these external providers. The Verizon 2019 data breach investigations report reveals that the financial sector experienced a high number of data breaches compared to other industries in 2018. When data is transferred between two entities, the involvement of third parties can potentially weaken the security defenses of financial institutions.

Third-Party Risks

Financial institutions often rely on third-party vendors or service providers, creating potential vulnerabilities if these partners have weak security measures.

- **Users' Compliance**

As emphasized by Security Intelligence report (2016), compliance is a crucial factor in addressing cybersecurity concerns within financial organizations. With the growing number of data breaches, financial institutions face the challenge of various perspectives on users' compliance with related to data protection and privacy Information system security policies.

Therefore, failure to comply with security policies and standards can expose financial institutions to legal and reputational risks, as well as potential cybersecurity vulnerabilities.

- **Internal or Insider vulnerabilities/gaps**

Insider vulnerabilities pose a significant cybersecurity threat in the financial sector and other organizations. These vulnerabilities occur when users or employees within an organization unknowingly expose organizational data to potential attacks. According to IBM's 2019 X-Force Intelligence Index, insiders were found to fall for phishing emails and websites in more than two-thirds of the cases studied, accounting for 29% of the attacks. Improper configuration of applications and systems, as well as misconfigurations of network devices, are also common causes of insider vulnerabilities.

- **Gaps in technology itself**

According to a ZDNet report (2018), financial institutions' websites are at a high risk of being hacked. The report revealed that 80% of the evaluated financial sites were vulnerable to cross-site scripting attacks. As a result, it is crucial to conduct vulnerability assessments on applications and systems before they are deployed live.

As a result of the security vulnerabilities mentioned earlier, the financial sector is particularly vulnerable and suffers to the following types of security attacks:

- **Phishing attacks**

Phishing is a common type of cybersecurity attack that aims to obtain sensitive user data, including login credentials and credit card numbers. This attack involves an attacker deceiving an unsuspecting victim by presenting them with a fake spoofed email or link. Once the victim interacts with the phishing email or link, malware is installed on their device, which can lead to data encryption as part of a ransomware attack.

- **Ransomware**

Ransomware is a form of malicious software that encrypts the files of its victims, rendering them inaccessible. Financial institutions are frequently targeted by ransomware attacks due to the potential for significant financial gains. In fact, according to a 2019 report by Kaspersky Labs, the financial services industry is the second most targeted sector for cyber-attacks, following the

healthcare industry. The primary objective of ransomware attacks is financially motivated, aimed to gain money from the victims.

Once the victims are able to make the requested payment, the attacker will then provide them with the decrypting key for their files/data, allowing them to regain access to their encrypted data.

- **Insider Attacks**

Insider or internal threats, privacy concerns, responsibility, and trust play a significant role in cybersecurity across various industries, including the financial sector. Yaseen (2016) emphasizes the vulnerability of financial institutions to insider threats due to the sensitive nature of the information they handle and their heavy dependance on information technologies. He also emphasizes that the financial industry is particularly impacted by cases of fraud and intellectual property theft committed by malicious insiders.

- **Distributed Denial of Service (DDoS)**

The financial sector is widely recognized as a main target for distributed denial-of-service (DDoS) attacks, which can occur at both the network and application layers. These attacks are employed as a means to disrupt financial services, as indicated by the EMEIA (Europe, Middle East, India & Africa) Cyber Centre of Excellence report. The growing emergence of botnet attacks is contributing to the increasing complexity of these DDoS attacks. According to Akamai (2018), state of the Internet report, DDoS attacks seen a significant increase of 16% from November 2017 up to April 2018.

- **Social Engineering Attacks**

Cybercriminals manipulate individuals through psychological manipulation or impersonation to gain unauthorized access to systems or sensitive information.

- **Weak Authentication Measures**

Inadequate password policies or failure to implement multi-factor authentication can leave accounts vulnerable to unauthorized access.

In conclusion, in the above as mentioned global cybersecurity attacks are also obvious within the financial institutions sector, particularly in banks. According to Kaspersky (2020), banks experience approximately 2.9 percent of malware attacks worldwide, making the financial sector

to be the third most targeted in terms of malware attacks. The most predominant types of fraud encountered by financial institutions such as credit card fraud, computer fraud, and manipulation of Automated Teller Machines (ATMs) fraud, as stated by Kaspersky.

2.4. Information System Security Prevention Mechanisms

Information system security prevention mechanisms refer to measures and techniques implemented to proactively protect information systems from potential threats and vulnerabilities. These mechanisms aim to prevent unauthorized access, data breaches, and other security incidents.

One commonly used prevention mechanism is the implementation of firewalls. Firewalls act as a barrier between internal networks and external networks, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules (Kizza, 2019). They help prevent unauthorized access and protect against network-based attacks.

Another important prevention mechanism is the use of encryption. Encryption involves converting sensitive information into unreadable ciphertext, which can only be decrypted with the appropriate encryption key (Whitman and Mattord, 2019). Encryption ensures that even if unauthorized individuals gain access to the data, they cannot understand or use it.

Access control mechanisms are also crucial in preventing unauthorized access to information systems. These mechanisms involve implementing user authentication, authorization, and accountability measures (Kizza, 2019). By ensuring that only authorized users can access sensitive information and perform specific actions, access control mechanisms help prevent unauthorized activities and potential security breaches.

Additionally, regular system updates and patch management are essential prevention mechanisms. Keeping software and systems up to date helps address known vulnerabilities and weaknesses, reducing the risk of exploitation by attackers (Whitman and Mattord, 2019).

Overall, a combination of prevention mechanisms, including firewalls, encryption, access control, and regular updates, etc is necessary to establish a strong security posture for information systems.

2.6. Information System Security Policy (ISSP)

The Information Systems Security Policy (ISSP) refers to a collection of formalized procedures, policies, guidelines, rules, roles, and responsibilities that employees are required to follow in order to safeguard and effectively utilize their organizations' information and technology assets. Various previous studies have explored the factors that influence employee compliance with ISSP. Moody et al. (2018) have proposed a comprehensive model for information security compliance that examines different factors that contribute to compliance. Additionally, Cram, DArcy, and Proudfoot (2019) conducted a meta-analysis that categorized 401 independent variables as predictors of ISSP compliance behavior.

Moreover, the information security policy can be defined as a set of policies, regulations, rules, and practices that govern how an organization manages, protects, and distributes information (Nieles et al., 2017). It serves as the foundation for all information security plans, designs, and implementations within the organization (Yung et al., 2020). Given the reliance of organizations on information systems, it becomes imperative to manage the associated risks effectively (Bulgurcu et al., 2010). While organizations often rely on technical security solutions to mitigate information security threats, it is important to recognize that technology alone cannot fully address security risks. Achieving success in information security requires investment in both technical and socio-organizational resources. According to NIST SP800-14 (National Institute of Standards and Technology, 1996), there are three levels of information security policy. The first level is the System Specific Security Policy), which comprises specifications for management operations and technical operational specifications used during system configuration and maintenance. The second level is the Issue-Specific Security Policy (ISSP), which provides guidance to employees on the correct use of various technologies and processes implemented by the organization for routine operations. The highest level is the Enterprise Information Security Policy (EISP), which serves as the overarching policy based on an organization's mission, vision, and direction, encompassing the general enterprise security policy, organizational security policy, IT security policy, or information security policy (NIST, 1996).

In the past decade, security concerns have become a top priority in the field of information systems (IS) management. It has been observed that relying solely on security tools and mechanisms is insufficient to ensure adequate protection. Instead, these tools and mechanisms should be

integrated into a comprehensive IS security policy, which consists of a structured set of principles, strategies, and detailed guidelines for safeguarding an IS. Traditionally, security issues have predominantly been addressed through technical solutions, such as intrusion detection and access control mechanisms. However, it is important to recognize that IS should not be solely evaluated from a technical perspective. IS encompasses various elements, including information, software, hardware, processes, and people, all of which interact with each other (Eloff and von Solms, 2000).

In order to promote the prevention of sensitive information disclosure and unauthorized use of software or hardware in IS operations, it is necessary to implement management activities such as audits and controls, as well as human resource development activities like further education. While technical methods play a crucial role, it is important to note that relying solely on technical measures is insufficient to ensure IS security (Eloff and von Solms, 2000).

2.7. Users' Compliance on Information System security Policy (ISSP)

Information system security compliance refers to the adherence of employees to an organization's information security policies and procedures when utilizing the information system (Alkalbani et al., 2017). When employees comply with the Information Systems Security Policy (ISSP), it signifies that they are following the policy while accessing and using information systems and engaging in communication with colleagues both within and outside the organization (Bulgurcu et al., 2010). The level of employee compliance with information security policies indicates the effectiveness of the implemented policies and procedures, while non-compliance suggests a rejection of the ISSP that has been put in place. It is crucial for the ISSP to strike a balance between ensuring security and not hindering employees' ability to carry out their daily tasks (Antoniou, 2015).

Promoting information security within organizations can be achieved by emphasizing the roles and responsibilities of individuals involved (Herath and Rao, 2009). When employees have clearly defined roles and responsibilities, they are more likely to proactively take measures to ensure information security (AlKalbani et al., 2015). Herath and Rao (2009) highlight the significance of information security accountability in organizations to ensure compliance. Human factors continue to be seen as a vulnerable aspect in safeguarding personal data. Awareness plays a crucial role in addressing this, as it is considered one of the most important privacy safeguards. Users who lack awareness and knowledge may unknowingly put their personal information at risk. Insufficient

awareness of information security compliance can have a negative impact on users' behavior, as they may unknowingly place trust in non-compliant or unreliable organizations. The effective methods of promoting information security compliance awareness are still being explored and developed in practice.

Organizational factors play a significant role in information security compliance within organizations. Drawing upon established theories like the Technology-Organization-Environment (TOE) theory (Tornatzky et al., 1990), the influence of socio-organizational factors on the implementation of information security compliance is studied. According to the TOE theory, the adoption and implementation of technological innovations in organizations are influenced by the technological, organizational, and environmental contexts in which they operate. The organizational context encompasses characteristics such as organizational structure, communication processes, and top management support, all of which contribute to promoting information security compliance. Well-developed organizational initiatives, such as active involvement of top management, directly impact employee behavior in adhering to information security standards and policies. Additionally, organizational processes play a crucial role in effectively managing information security controls.

Insufficient support from management in promoting compliance with information security policies has been identified as a common reason for the inadequate implementation of such policies in organizations (Kolkowska and Dhillon, 2012). Enhancing information security compliance within organizations can be achieved through the promotion of information security awareness (McIlwraith, 2006). Information security awareness programs serve as effective means to improve compliance by enhancing users' knowledge and understanding of security policies and mechanisms within the organization (Puhakainen & Siponen, 2010). For instance, the presence of information security awareness programs significantly influences employees' beliefs regarding the benefits of compliance and the costs associated with non-compliance. demonstrate that the utilization of information security awareness and training programs can reduce the misuse of information security policies and procedures, as well as increase users' ability to avoid information security risks and threats within organizations.

The technological context of an organization refers to the reliability of security technologies in meeting information security policies and standards. Technology plays a crucial role in enabling

secure transactions, safeguarding access to information, and protecting against hacking (Venter and Eloff, 2003). The adoption of appropriate security technologies that align with security requirements instills trust among stakeholders and contributes to improved information security compliance (Moynihan, 2004). For instance, evaluating the effectiveness of security technologies like digital signatures can be instrumental in enforcing security compliance. Technological capabilities can enhance the smooth functioning of information systems by reducing security risks and minimizing costs within organizations. Ajzen (1991) explores the use of role-based access control systems to enforce information security policies within organizations. By employing suitable security technologies, organizations can effectively enforce policies, monitor and flag violations, and strengthen information protection for enhanced information security (Venter and Eloff, 2003). These previous studies demonstrate the impact of security technologies on the implementation of information security policies within organizations.

In conclusion, Users' compliance refers to to the practice of following an organization's established security policies, procedures, guidelines, and specifications. Ensuring users' compliance and adherence should be an obligatory and mandatory requirement for organizations, particularly those operating in the digital financial sector.

2.8. Information security best practices

Information security practices are critical for organizations to safeguard their sensitive information and protect against potential threats. One essential practice is the implementation of access controls, which restrict unauthorized access and ensure that only authorized individuals can access sensitive information. This includes mechanisms such as user authentication, authorization, and encryption (Whitman & Mattord, 2019). Additionally, conducting regular risk assessments and implementing appropriate controls based on the findings is crucial in identifying vulnerabilities and mitigating potential risks (ISO/IEC, 2022). Security awareness training programs play a vital role in educating employees about information security best practices and raising awareness about potential threats (ISO/IEC, 2022). Incident response and management procedures are also essential to detect, respond to, and recover from security incidents or breaches effectively (Whitman & Mattord, 2019). Regular system updates and patch management help address known vulnerabilities and protect against potential exploits (ISO/IEC, 2022). Lastly, implementing robust data backup

and recovery mechanisms ensures that data can be restored in the event of data loss or system failure (Whitman & Mattord, 2019).

2.9. Cybersecurity Policy and Strategy in Ethiopia

In Ethiopia, the Information Network Security Agency (INSA) initially developed the National Information Security Policy in 2011. Recently, in 2021, they have updated the Cyber Security Policy and Strategy (CSPS).

Additionally, the Ministry of Finance (MoF) has developed its own Cyber Security policy in 2023, aligning with the national information security policy and framework. Despite the formulation of a computer crime law by INSA in 2016, the absence of comprehensive cybersecurity legislation, rapidly advancing technologies, legal uncertainties, and jurisdictional challenges have created a lack of guidance for cybercriminals and hindered the effective implementation of existing laws. Consequently, this has led to a significant number of cybercriminals operating freely within the country. For instance, INSA reported defending against six million cyber-attacks within a six-month period in 2022.

To ensure effective coordination and management of national cybersecurity incidents, Ethiopia has recently established the Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CER2T). This centralized defense mechanism serves as a focal point for reporting and handling cyber incidents within the country. Consequently, there is a pressing need for a cybersecurity framework that can provide guidance and support in safeguarding Ethiopia's cyberspace.

As cyber threats continue to rise, the security of sensitive data and organizations is increasingly at risk. The absence of adequate cybersecurity measures and adherence to best practices makes companies vulnerable targets for hackers. Kaspersky (2020) reports that approximately 2.9 percent of global malware attacks specifically target financial institutions. Therefore, it is necessity to establish a cybersecurity framework to address this escalating threat of cybercrimes.

The financial industry regulatory authority is currently undertaking compliance initiatives to meet security standards, particularly the Payment Card Industry Data Security Standard (PCI-DSS). Additionally, financial institutions have the flexibility to choose which cybersecurity standards they wish to implement, as there is no specific requirement mandating a particular standard.

Financial institutions must adhere to relevant industry information security standards and adopt internationally recognized best practices as appropriate. This ensures that regulated entities can effectively identify, assess, and mitigate the risks and damages associated with cybercrime. It is also essential for financial institutions to ensure that their staff, customers, and suppliers are aware of the risks associated with cybercrime. This is achieved through comprehensive staff training programs and awareness campaigns targeting clients and suppliers. For instance, the Ministry of Finance (MoF) in Ethiopia, as being a financial institution at the ministerial level, has rented a training room at the 5killo university campus to provide foundational awareness training on general security to its employees, customers, and suppliers. Overall, the financial sector acknowledges the significant challenge posed by cybercrime.

Furthermore, cybercrime poses the risk of unauthorized disclosure of information and the potential loss of sensitive data, which can significantly impact a company's competitive advantages with against other businesses (Mohammed, 2018). As a result, it is crucial to develop robust cybersecurity frameworks and implement best practices, not only for the general public but also specifically for financial institutions.

Companies become vulnerable targets for hackers due to the absence of adequate cybersecurity frameworks, measures and best practices (Li, 2017). Law enforcement agencies should implement a range of measures to combat cybercrime. However, Ethiopia is behind in terms of cybersecurity international trends and policies, lacking the necessary technical and financial capabilities to effectively address these threats. Hence, the implementation of a cybersecurity framework becomes crucial as it will significantly mitigate the risks associated with cybercrimes.

2.10. Existing Cybersecurity Frameworks, Policies, Best Practices and Standards

2.10.1. Overview

The increasing occurrence of cyber threats targeting financial institutions has emphasized the importance of enhancing cybersecurity in the financial sector. Consequently, cyber risk has become a concern for everyone. Cyber risk refers to the operational risks associated with information and technology assets, which can have adverse effects on the confidentiality, availability, and /or integrity of information and information systems (Bouveret, 2018). Therefore, cybersecurity involves safeguarding information and technology assets, such as network devices and servers, from emerging risks and cyberattacks.

Organizations recognize the importance of adopting international cybersecurity standards or best practice frameworks to effectively manage and guide their cybersecurity efforts. In order to a cybersecurity conceptual framework to be successful, it is crucial to consider industry standards and best practices (Kritzinger & Von Solms, 2012). Several international standards, frameworks, and best practices have been developed and tailored for cybersecurity purposes. Notable examples include (i) NIST cybersecurity framework for critical infrastructure by the National Institute of Standards and Technology (2018), (ii) the Committee on Payments and Market Infrastructures (CPMI) cybersecurity framework (Crisanto & Prenio, 2017), (iii) the ISO/IEC 27001:2013 Standards on Information Security Management System (ISO, 2013), (iv) the Center for Internet Security (CIS) framework (Center for Internet Security, 2018), and (v) the framework for the Governance of Information Security in the Banking System (Ula, Ismail, & Sidek, 2011). The following sections will provide a detailed review of these frameworks.

2.10.2. National Institute of Standards and Technology Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has developed a framework that aims to enhance cybersecurity for critical infrastructure in the United States. Critical infrastructure refers to assets or systems that are essential for maintaining critical national functions. This includes physical resources, IT facilities, services, networks, and infrastructure that are vital for national health and security, public safety, the economy, and the well-being of citizens (Chochliouros et al., 2015). It is obvious that the financial sector and institutions are integral parts of critical infrastructure as they heavily rely on information and communication technology (ICT) as a means to conduct their business. They play a significant role in providing essential support services for the economy and society, contributing to the country's Gross Domestic Product (GDP).

Therefore, ensuring the security of their systems is crucial for the proper functioning of the market (National Institute of Standards and Technology, 2018).

In response to the executive order 13636 issued by the United States President on February 12, 2013, the National Institute of Standards and Technology (NIST) was asked to develop an effective cybersecurity framework to protect critical infrastructure (Order, 2013). As a result, the NIST cybersecurity framework was created and published. This framework is designed to assist organizations of all sizes, sectors, and types in managing their cybersecurity risks by aligning them with their overall business risks. By focusing on business objectives and drivers, the NIST

framework helps organizations identify, assess, and manage cyber risks. It is important to note that the framework is not limited to critical infrastructure organizations but is applicable to any organization in any sector or community, including both the private and government sectors, as there are currently no defined cybersecurity best practices (National Institute of Standards and Technology, 2018).

The NIST cybersecurity framework has three main components: the framework core, profiles, and implementation tiers. The framework core comprises a set of cybersecurity activities that are intended to achieve the desired cybersecurity outcomes for critical infrastructure sectors. It consists of five key functions: identify, protect, detect, respond, and recover, as shown in figure 2.1. The framework profiles describe the specific cybersecurity outcomes an organization wants to achieve based on its particular business needs, using categories and sub-categories. The implementation tiers indicate how organizations manage cybersecurity risks and establish procedures to control those risks (National Institute of Standards and Technology, 2018).

The NIST Cybersecurity Framework is depicted in Figure 2.1 as following.

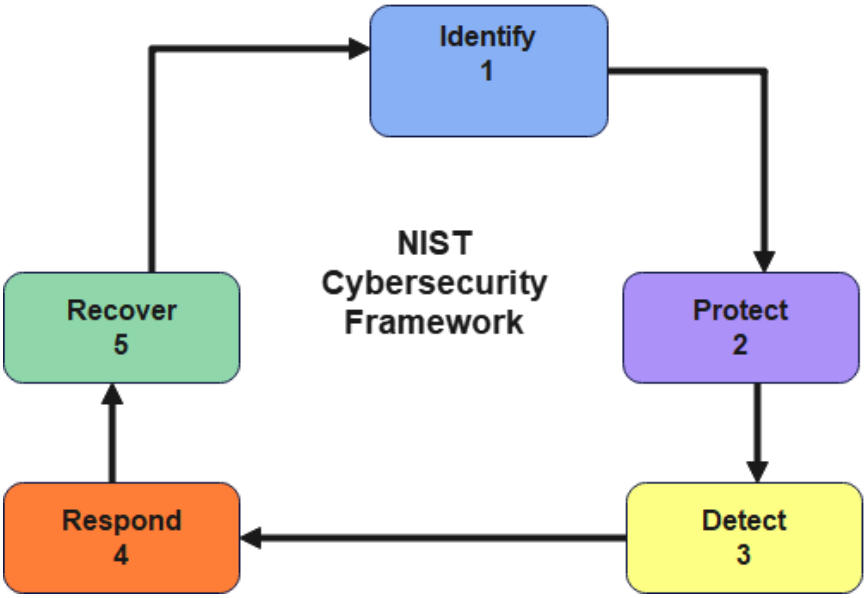


Figure 2-1: *NIST Cybersecurity Framework*

The NIST cybersecurity framework is well-suited for the financial sector. Because the financial sector operates within the international financial system principles, it is critical to understand the international definition of critical infrastructure and collaboration with international regulators. Clearly, finance has a complex regulatory environment with numerous international compliance

standards like PCI-DSS; it is crucial for the financial sector to adopt a comprehensive cybersecurity framework. The NIST cybersecurity framework allows organizations to determine their own level of precaution and provides flexibility to address unique threats, vulnerabilities, and risk factors. This adaptability makes the NIST framework suitable for implementation in the financial sector, as it can be tailored to meet specific industry needs and compliance obligations.

The use of this voluntary framework helps in improving the cybersecurity of the critical infrastructure and guide individual organizations in increasing the cybersecurity posture, identify and prioritize scenarios for improving IT security through risk assessment, target state and assess progress in cybersecurity (Teoh, Mahmood, & Dzazali, 2017). Thus, in the financial sector, the framework could enhance cybersecurity resilience and provide improved safeguards for the financial institutions' client accounts and data.

By implementing this voluntary framework, organizations can enhance the cybersecurity of critical infrastructure and improve their overall cybersecurity posture. It assists in identifying and prioritizing scenarios for enhancing IT security through risk assessment, setting target goals, and evaluating progress in cybersecurity (Teoh, Mahmood, & Dzazali, 2017). As a result, in the financial sector, adopting this framework has the potential to strengthen cybersecurity resilience and provide better protection for client accounts and data held by financial institutions.

2.10.3. ISO/IEC 27001:2013 Standards on Information Security Management Systems (ISMS)

The International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27000 series is a significant technical standard in the cyber and information security community ISO/IEC 27001:2013 specifically provides guidance on implementing an Information Security Management System (ISMS) within organizations to protect their information assets. This standard has been widely adopted globally across many types of organizations. Implementing an ISMS as outlined in ISO/IEC 27001 assists companies in putting countermeasures in place to address information systems vulnerabilities. Overall, the ISO/IEC 27000 standards are an important tool used internationally to manage information security risks.

The ISO/IEC 27001 standard encompasses risk management, security management, governance, and compliance. It assists organizations in establishing the required people, procedures, and

technologies to ensure effective security and risk management. A successful information security management system (ISMS) under the ISO/IEC 27001:2013 standard necessitates mandatory information security commitments from all stakeholders and senior management within an organization. By adopting this standard, organizations can take a proactive approach to security.

2.10.4 Center for Internet Security (CIS)

The latest version of the CIS controls, released in March 2018, includes twenty essential cybersecurity recommendations. These controls are comprehensive security best practices developed by IT experts from various sectors. They aim to mitigate cyber-attacks on systems and networks by providing in-depth defense strategies (Center for Internet Security, 2018). The continuous advancement of cyber defense is a response to significant data breaches, credit card compromises in financial institutions, privacy risks, intellectual property theft, and denial-of-service attacks. These challenges arise due to our digital and interconnected world, with billions of connected devices ranging from mobile devices and personal computers to Internet of Things (IoT) devices.

CIS offers cyber defenders access to security standards, recommended security controls, and best practices. It focuses on identifying the most critical risk areas that organizations should address to enhance their current security posture. The CIS controls prioritize the most essential and effective security activities that any organization can implement to provide top-class cybersecurity solutions, enabling them to prevent and respond to cyber incidents quickly. The primary objective of the CIS controls is to enhance the organization's knowledge and capabilities in preventing, detecting, and responding to cyber-attacks.

The CIS identifies five crucial principles for a robust cyber defense system: (1) leveraging offensive tactics to inform defensive strategies, (2) prioritizing security measures, (3) employing measurements and metrics to assess effectiveness, (4) implementing continuous diagnostics and mitigation practices, and (5) utilizing automation for improved efficiency. Version 7 of the CIS controls encompasses seven key principles and addresses the current cybersecurity threat landscape faced by all organizations. It is designed to align with other frameworks, such as the NIST Cybersecurity Framework, and offers adaptable, relevant, helpful, measurable, and flexible controls suitable for organizations of all sizes seeking to secure their systems and data.

2.10.5. A Framework for the Governance of Information Security in Financial System

According to Ula et al. (2011), safeguarding information has become crucial in the modern financial industry, as it is considered the most valuable asset that must be protected from internal/insiders' threats, external/outsiders' threats, and competitors. Clients have become increasingly concerned about their privacy, making security a top priority for financial institutions when delivering their services. In response to this, various cybersecurity frameworks have been developed and widely adopted. Authors define information security governance as a structure, relationship, and process that involves implementing frameworks for governing information security. The implementation of information security governance typically entails aligning responsibilities within the organizational hierarchy.

The initial design of the proposed Information Security Governance (ISG) framework incorporates best practices and components from various existing governance frameworks. This integration includes frameworks such as the Federal Financial Institutions Examination Council (FFIEC), Control Objectives for Information and Related Technology (COBIT), International Organization for Standardization (ISO) 27002, Payment Card Industry Data Security Standard (PCI-DSS), Corporate Governance Task Force (CGTF), Information Systems Security Association (ISSA), and Corporate Information Security Working Group (CISWG). By incorporating elements from these diverse frameworks, the ISG framework aims to provide a comprehensive and robust approach to information security governance.

The ISG framework can serve as a foundation for governing information security in the financial sector. It allows for the establishment of standards and the implementation of controls to safeguard financial information assets against cybersecurity threats. It is important to note that none of the frameworks mentioned in the study cover all aspects of information security governance. For example, the PCI security standard is specifically tailored to the operational level, while frameworks like ISO 27002 or COBIT primarily provide technical practice security guidelines focused on the configuration and operation of IT systems, with indirect consideration for data security (Ula et al., 2011). The ISG framework encompasses three levels**:** strategic**;** tactical (operational); and technical levels those enabling comprehensive coverage of information security

governance across different organizational levels. The ISG framework proposed by Ula et al. (2011) is depicted in the following Figure 2.2.

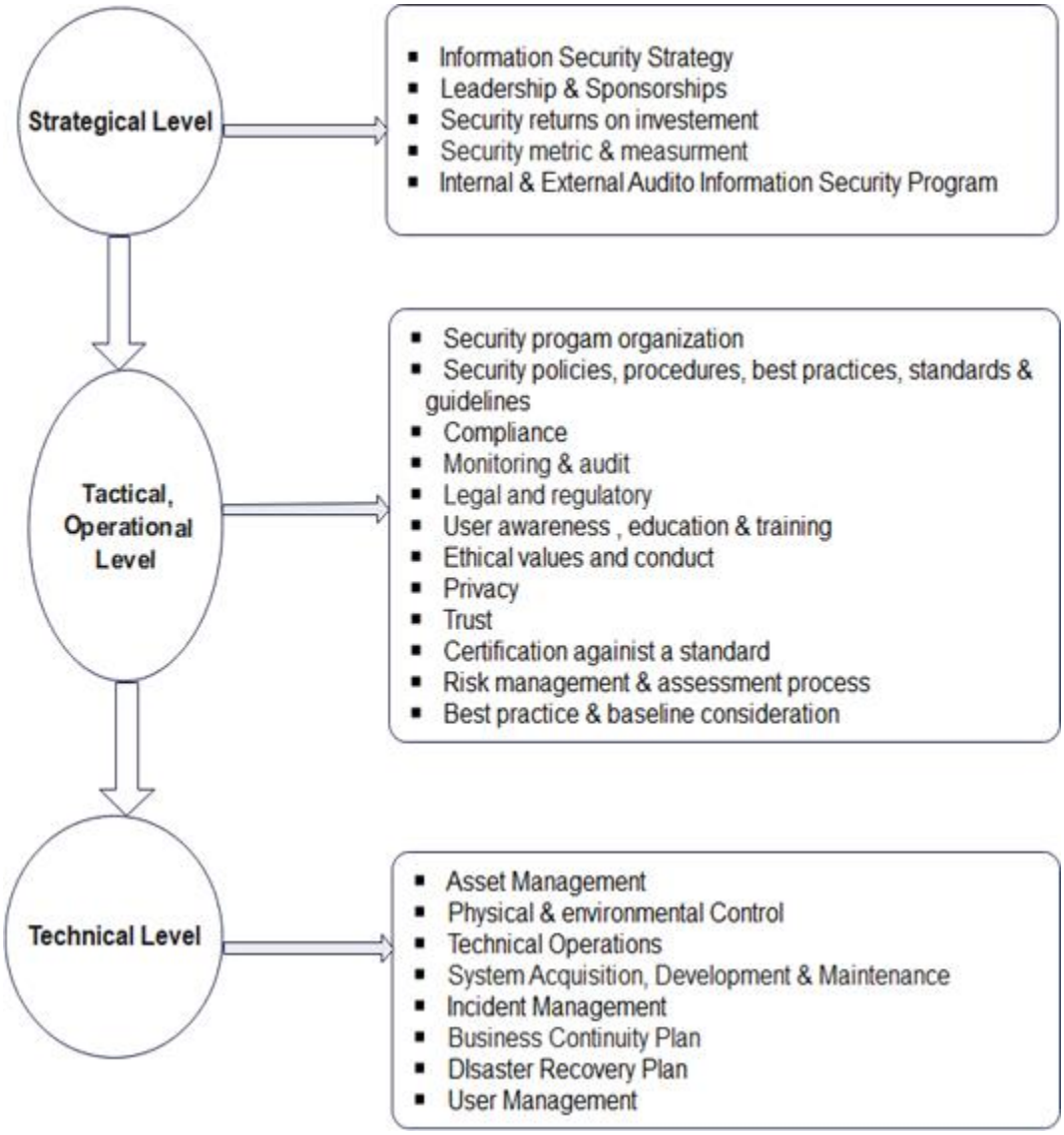


Figure 2-2: *The ISG framework*

Unfortunately, cybersecurity frameworks vary from country to country due to differences in the environment and specific circumstances. In the case of Ethiopia, as a sovereignty nation, it is necessary to develop a framework that addresses the unique cybersecurity needs of its citizens and financial institutions. Ethiopia has already established an official national cybersecurity strategy through the Ethiopian Information Network Security Agency (INSA) in 2022. There is well-established computer crime law in 2016, Ethiopia has taken steps towards cybersecurity preparedness by establishing the Ethiopian Emergency Readiness and Response Team (Ethio-

Cer2t). This team, under the control of INSA, is responsible for managing and reporting national cyber incidents, ensuring a centralized approach to addressing cybersecurity incidents in the country.

2.11. Review For Related works

The previous studies have focused on various factors influencing Information System Security Policy (ISSP) compliance, including organizational, social, individual, and technological factors. Temtim and Alpha (2021) identified four organizational factors that shape employees' compliance behavior with information security policies in Ethio-telecom company. Their findings highlighted top management support/commitment, accountability, awareness, and training as the most influential organizational factors, while audit and monitoring had less impact. Other study also identified significant factors that affect information security compliance. The factors are coercive factors (rules & regulations), mimetic factors (security benefits), and senior management commitment, as well as socio-organizational factors (AlKalbani et al., 2017).

Bulgurcu et al. (2010) investigated individual factors that influence employees' compliance with ISP requirements in terms of protecting the organization's information and technology resources. They found that employees' attitudes are influenced by their perception of the benefits and costs of compliance, including intrinsic and extrinsic costs.

The limitations of the study conducted by Bulgurcu et al. (2010) for my research questions are as follows:

i. The study focuses on individual factors that influence employees' compliance with information security policies (ISP) requirements, rather than specifically addressing the main information system security threats at the Ethiopian Ministry of Finance (MoF) financial institution's cyberspace. It may not directly provide insights into the specific threats faced by the MoF.

ii. The study does not directly investigate the implemented information system security prevention mechanisms in the MoF context. It primarily examines employees' attitudes towards compliance, rather than the specific preventive measures implemented by the MoF.

iii. The study does not explicitly aim to develop an information system security framework. While it examines individual factors influencing compliance, it does not provide a comprehensive

framework that addresses the specific needs and requirements of the MoF in terms of information system security.

Therefore, while the study by Bulgurcu et al. (2010) provides valuable insights into employees' compliance with ISP requirements, it may have limitations in directly addressing my research questions related to information system security threats, prevention mechanisms, and framework development at the Ethiopian MoF financial institution.

The Qatar Ministry of Transport and Communications (MOTC) Cyber Security Policy and Standards (2018) define several security control policies for Bring Your Own Devices (BYOD). These policies include acceptable use, provisioning, management, encryption, and audit logging. These policies aim to ensure compliance with laws and regulations, the use of genuine and licensed operating systems and applications, access control, encryption of government data, and logging of all relevant events.

User adherence to BYOD security policies is influenced by various factors. Bhagat et al. (2020) examined the adoption of BYOD policies from the perspective of employees' moral beliefs, subjective norms, and self-regulation. They found that social connections formed in the work environment significantly influence attitudes towards compliance and subjective norms, which in turn positively impact employees' ISSP compliance. These socio-organizational and psychological factors play a role in promoting employees' compliance with ISSP in the workplace (Ifinedo, 2014).

Overall, these studies highlighted the importance of considering organizational, individual, social, and technological factors in developing effective information security frameworks and promoting compliance with ISSP. Understanding these factors can help organizations design and implement appropriate policies, provide necessary support and training, and foster a culture of information security awareness and responsibility among employees.

2.12. Research Gaps

The previously discussed information security and cybersecurity guidelines, standards, and frameworks cannot be universally applied to all financial sectors and countries due to the specific and unique needs of each financial institution. These standards and frameworks vary from country to country due to differences in the environment, situational factors, and the knowledge and skills

required for implementation. As a sovereign nation, Ethiopia recognizes the importance of addressing its cybersecurity needs and has taken steps to establish a structure capable of meeting the cybersecurity requirements of both its population and financial institutions.

Moreover, the literature review clearly indicated that most framework studies primarily focused on a limited set of cybersecurity features, including security policies, procedures, best practices, standards, guidelines, security programs, monitoring and compliance, user awareness, education and training, and risk management and assessment processes. However, these studies did not see the other crucial aspects such as human factors and cybersecurity simulations. As a result, there are gaps in their coverage and conceptualization of cyber risks, particularly in the context of the financial sector. These limitations hinder the applicability of existing frameworks in developing countries like Ethiopia.

The reviewed frameworks did not include components such as corporate governance, ethical conduct, trust, and auditor security programs, despite the recognition of their importance by various researchers in implementing information security controls within organizations (Ula et al., 2011). While the NIST framework incorporates corporate governance and the ISO standard addresses ethical conduct and auditor security programs, it remains unclear how these components can be effectively implemented in the Ethiopian context. The guidelines and implementation strategies for these components are primarily outlined within the compliance context of European countries, where enforcement of these standards is more severe compared to Ethiopia.

Furthermore, it is worth noticing that some of the existing cybersecurity frameworks, best practices, and guidelines, such as NIST, CPMI cybersecurity framework, ISO/IEC27001, CIS, and the framework for the Governance of Information Security in the Financial System lack proper evaluation (Ula et al. (2011). Evaluating these frameworks and standards is crucial as it helps determine their usability and feasibility. Therefore, further research is necessary, involving key stakeholders from top management in the financial sector industry. Bringing together these stakeholders in Ethiopia's financial sector industry can effectively address cyber risks, established a theoretical foundation for cybersecurity, assess implementation feasibility in the financial sector, and develop methodologies for evaluating cyber threats to ensure long-term sustainability.

Hence, it is crucial for every financial institution to ensure that their employees, customers, and suppliers are well-informed about the risks associated with cybercrime. This highlights the

importance of developing an information system security framework specifically tailored for the financial sector. Such a framework would serve to unify processes and provide financial institutions with standardized requirements, making a significant contribution to the understanding of cyber risks and strategies in Ethiopia.

2.13. Chapter Summary

In today's digital age, information security has become a critical concern for organizations across various sectors. Developing a robust information system security framework is essential to safeguard sensitive data, protect against cyber threats, and ensure the confidentiality, integrity, and availability of information assets. This review aims to explored existing literature on the development of information security frameworks, highlighting key concepts, threats, attacks, and best practices.

The chapter provides a comprehensive overview of cybercrimes in the financial sector. In Ethiopia, various types of cyber-attacks are experienced, including computer fraud, social engineering, phishing attacks, viruses, worms, Trojans, ransomware, insider attacks, and DOS/DDoS attacks. The digital transformation within the financial sector industry has increased the potential attack surface, making it a key risk for cyber-attacks on financial systems. Financial institutions have become attractive targets due to the large amount of sensitive customer data they handle and their critical role in payment systems.

To mitigate this risk, financial institutions have implemented security measures such as incident response activities, training and awareness programs, asset management, third-party cyber risk management and so on. There are globally recognized information/cybersecurity standards and frameworks available for financial institutions to enhance their cyber resilience. These include the NIST cybersecurity framework, the CPMI cybersecurity framework, ISO/IEC 27001:2013 Standards on Information Security Management System, PCI-DSS, CIS, and a framework for the Governance of Information Security in financial systems.

However, the literature review revealed that the focus of existing framework studies primarily circles around a limited set of cybersecurity features, such as security policies, procedures, best practices, standards, guidelines, security programs, monitoring and compliance, user awareness, education and training, and risk management and assessment processes. Additionally, there is a lack of clarity on how these frameworks can be effectively implemented in the Ethiopian context.

This highlights the identified gaps in some existing information/cybersecurity standards and frameworks, as they did not adequately address essential components such as human factors, cybersecurity simulations, corporate governance, ethical conduct, trust, and auditor security programs.

These limitations identified in the literature review inform the proposed information system security framework that was discussed in Chapter 4 data presenting and analysis. The next chapter 3 will present the research methodology used to conduct this study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Introduction

This chapter focused on the research method of the study. The research paradigm was discussed in order to emphasize various aspects of this study. The research methodology refers to the general principles, guidelines and assumptions that shape how the research was carried out. This chapter described the whole research process such as research approaches, research design, sampling technique, data collection and data analysis methods applied in this research study.

3.2. Research Methodology

According to Creswell and Creswell (2014), research methodology refers to the overall approach or general guidelines to carrying out or to address a specific research problem. It includes the theoretical frameworks, philosophical perspectives, systematic data collection and analysis methods and techniques, as well as tools used in the research. Some examples of research methodologies are quantitative, qualitative and mixed methods

On the other hand, research design presents the specific plan, roadmap or blueprint that a researcher develops to conduct a specific study and to answer specific research questions. This includes details like the study population, data collection and analysis methods, techniques, measurement tools, etc.

In summary**,** research paradigm refers to the set of beliefs, assumptions, methodological approaches, which include different philosophical framework that show researcher's worldviews. It used as lens that shows how scientific inquiries are, designed, studied and carried out. The common research paradigms include positivism, interpretivism, critical theory (critical reality), and pragmatism.

3.2. Research Paradigm

A research paradigm encompasses the philosophical assumptions, shared beliefs, values, methodological approaches like quantitative, qualitative, and mixed methods research approaches as well as validity standards that provide a framework guiding scientific inquiry (Thanh & Thanh,

2015). It includes researcher's worldviews on the nature of knowledge and reality to investigate phenomena and construct knowledge. There are different commonly used paradigms, such as positivism, pragmatism, and interpretivism.

An evaluation of different research paradigms shows that positivist research is characterized by the formulation and testing of hypotheses using exact, objective metrics, and is most commonly linked with quantitative data (Muganda, 2010). Pragmatists, on the other hand, believe in external reality as they believe there are many ways of undertaking research. However, they do not think a single point of view can fully determine certain concepts since there may be multiple realities (Collis & Hussey, 2013). Thus, it is difficult to fully grasping causal relationships in pragmatism research. Pragmatism can combine both positivism and interpretivism paradigms, including the use of qualitative and quantitative methods.

Interpretivism is another common research paradigm. It involves the researcher being intimately and subjectively involved in what is being investigated (Muganda, 2010). Interpretivist research normally creates a deeper understanding of how social context influences by presenting a rich description of a particular context or case. Various paradigms encompass distinct worldviews, resulting in different assumptions about the nature of reality and knowledge. The interpretivist paradigm acknowledges that the creation of subjective meaning significantly shapes realities. Therefore, this interpretivist paradigm's assumptions align with qualitative research approach and descriptive investigations.

For this study, interpretivism were chosen as the research paradigm. This is due to the fact that its primary focus is on comprehending the social context of organizations, which includes knowing how the organization’s social processes are understood and how the individuals who work there interpret or perceive their information security practices (Muganda, 2010).

This study does not adopt positivism and pragmatism paradigms because its goals are not testing hypotheses. Rather, the research aimed to explore causal relationships related to information security practices such as threats, attacks and preventive mechanisms.

According to Gray (2014), interpretive studies typically follow an inductive approach and are frequently associated with qualitative methods of data collection and analysis. In the inductive process, researchers begin by collecting data with the aim of developing a theory or hypothesis.

Inductive techniques are intended to facilitate the interpretation of complex data by generating concise themes or categories from the transcribed data that collected by interviews, which is referred to as data reduction.

Interpretivism research, as described by Goldkuhl (2012), is characterized by the acquisition of knowledge through deep understanding. The primary focus of interpretivism is for the researcher to engage in understanding the topic under investigation. Therefore, this study used the interpretivism paradigm to gather data through interviews, document reviews and observations. The aim of this study was to analyze the different patterns of information security practices and assess the effectiveness of current cybersecurity frameworks.

As **Myers** (1997) states that the "... choice of research methodology and research design depends on the paradigm that guides the research activity, more specifically on beliefs about the nature of reality and humanity (ontology), the theory of knowledge underlying the research (epistemology), and how that knowledge can be obtained (methodology)". So, without choosing a paradigm as a first step, there is no basis for choosing methods or research design.

In conclusion, this study used interpretivist paradigm. The aim of this research was to develop an information security practices framework and assess the existing security practices at the Ministry of Finance (MoF). To accomplish this, the primary data collection methods used in this study were semi-structure interview, document reviews, and observation check list.

3.3. Research Design

The qualitative research method is characterized as a process that uses inductive data analysis to gain insight knowledge and beliefs of participants regarding a particular problem or issue, by identifying patterns or themes (Lewis, 2015). Unlike focusing solely on the what, where, when, or who, qualitative research approaches investigate into the reasons and mechanisms behind decision-making (Creswell & Poth, 2017).

According Gray (2014) stated that qualitative research offers various methods, including observation, interviews, surveys, content and thematic analysis to carried out different research needs. This method allows researchers to gain a comprehensive understanding of the research study, and making it well-suited for this study. In this particular study, semi-structured interviews were conducted as they are non-standardized and commonly used in qualitative analysis. The

utilization of qualitative research methods in this study is essential to acquire in-depth knowledge to propose research framework.

To examine different information security practices and assess the effectiveness of existing cybersecurity frameworks in the Ministry of Finance (MoF), a qualitative research design incorporating semi-structured interviews are used. This approach facilitated a comprehensive understanding of the current state of cyber maturity in the MoF and identified areas that require improvement. Semi-structured interviews are selected as the most suitable strategy for this study due to their flexibility asking the respondents questions in details and allowing the interviewer to to have deeper understanding about the research (Doody & Noonan, 2013).

Qualitative data is collected by conducting interviews with technical domain experts within the Ministry of Finance (MoF). These interviews and discussions involve both experts and managers in order to gather qualitative data.

This study uses a case study research design to explain information security practices, evaluate the current information security framework, and then propose a new framework. In order to effectively address the research problems, and achieve the research objectives, the study was designed using the following research process (See Fig. 3-1).

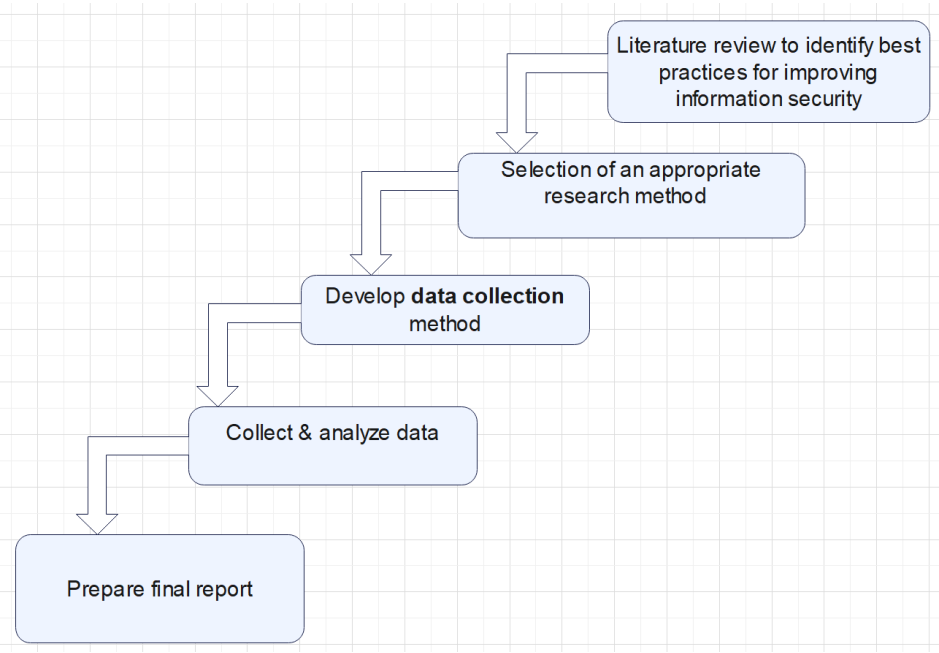


Figure 3-1: *Research Design process*

When the research is intended to create an artifact, researchers use design science research methodology. As stated by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007), "design science research is a research approach that focuses on creating and evaluating IT artifacts with the purpose of resolving specific organizational problems. It involves a systematic and rigorous process of designing artifacts to address observed issues, making research contributions, evaluating the designs, and effectively communicating the results to the relevant audiences" (p.6).

In order to address research objective 3, the researcher used the design science research methodology (DSRM) for Information Systems research, as proposed by Peffers et al. (2007). This methodology will guide the process of creating an artifact, specifically an information security framework, that is specifically tailored to address the cyber threat problems faced by the Ministry of Finance (MoF). The DSRM approach emphasizes the development of practical solutions to real-world problems, ensuring that the resulting artifact effectively addresses the unique cybersecurity challenges within the MoF context.

The design science research methodology by Peffers et al. (2007) consists of six steps, as shown in Figure 3-2.

Figure 3-2: *A design science research methodology for Information Systems research*

Descriptions of the six steps of research design methodology:

i. Problem identification and motivation

According to Kaspersky (2020), financial institutions globally face a significant threat from malware attacks, with approximately 2.9% of such attacks targeting these institutions. Despite the Ministry of Finance's (MoF) Cybersecurity unit having established a department structure, currently there is no officially recognized cyber security or information security framework in place to guide and improve information security practices and protect financial data sharing such

as the nine modules of Integrated Financial Management Information System (IFMIS) and many other public financial data. This absence is due to a lack of appropriate governance, supporting systems, procedures, and processes for effectively managing cyber risks associated with financial data sharing. Therefore, there is a need to develop a cyber security framework that can provide guidance and ensure the security of financial data sharing who utilizes MoF's financial public data services. The design of this framework was performed by an assessment of various information security practices and an evaluation of existing cyber security frameworks.

ii. Definition of the objectives for a solution

The objective is to develop a cybersecurity or information security framework that will provide guidance to the Ministry of Finance (MoF) for safeguarding financial data sharing. However, there are concerns regarding the adoption of international cybersecurity frameworks and standards, as there may be differences in the environmental and capability contexts. Additionally, security regulations vary from country to country. This emphasize the need for a cybersecurity framework that is specifically tailored to address the unique requirements and challenges faced by the MoF, ultimately reducing the threat of cybercrimes.

iii. Design and development

The assessment of various cybersecurity best practices, security policies, procedures, and existing framework, literature was conducted to evaluate the implementation of a cybersecurity framework. While these reviewed standards and frameworks offer significant benefits to financial institutions, they still show some level of incompleteness. To gain a comprehensive understanding of the current state of cyber maturity and identify areas for improvement within the Ministry of Finance (MoF), semi-structured interviews are conducted. These interviews help assess the different patterns of information security practices and evaluate the existing cybersecurity frameworks in place. By utilizing this approach, the researcher is able to design a framework that addresses the identified gaps and enhances the cybersecurity posture of the MoF.

iv. Demonstration

The developed framework was applied and tested in the context of the Ministry of Finance (MoF) to showcase its practicality and effectiveness. This case study will serve as a demonstration of the feasibility and efficacy of the framework within the specific context of the MoF.

v. Evaluation

The framework will undergo evaluation by cybersecurity experts within the Ministry of Finance (MoF) who possess domain expertise in the field. This evaluation process is conducted with the specific objective of obtaining verification regarding the accuracy and effectiveness of the framework. The input and feedback from these experienced professionals will provide valuable insights into the performance and suitability of the framework in addressing the cybersecurity needs of the MoF.

vi. Communication

The last phase involves the dissemination of the developed framework. Additionally, the findings and contributions of this study was shared through peer-reviewed scholarly publications and reported in a journal article. This ensures that the knowledge and insights gained from this research are shared with the academic community and other interested stakeholders.

In conclusion, in this study, data collection methods such as semi-structured interviews, document review, and observation checklists are used. These methods are chosen to ensure the validation of data through triangulation, thereby enhancing the credibility and reliability of the findings.

3.4. Data Collection

Qualitative research data collection methods commonly used in an interpretivist research paradigm which include interviews, focus groups, discussions, document reviews, observation that used for later content and thematic analysis. These methods allow for an inductive analysis approach and are highly valuable in addressing the initial research question(s) and ultimately achieving the research objectives. To achieve these objectives, multiple data collection tools are used as following.

There are various data collection methods available for interpretive research, including document reviews, observations, focus groups, discussions, and interviews. Focus group discussions are a specific type of data collection technique where a small group of participants, typically ranging from four to twelve individuals, come together to interact and engage in discussions. The focus groups are often chosen due to their ease of organization and cost-effectiveness, although their suitability for achieving the research goals may vary (Acocella, 2012).

According to Gray (2014), observations involve systematically reviewing and recording participants' actions, followed by the analysis and interpretation of the observed events. This method enables researchers to eliminate subjective bias and gather information about current occurrences. However, observations have limitations, such as providing limited information and being prone to unforeseen factors that can interfere with the observation process (Kothari & Garg, 2014). Observations are commonly employed in studies refer to behavioral sciences.

Another commonly used data collection method in interpretive research is the structured or semi-structured interview. In structured interviews, all participants are asked the same set of questions, ensuring consistency in the context of the interview (Gray, 2014). Structured interviews offer the advantage of using a detailed interview guide, allowing the researcher to control the topics and format of the interview. However, the strict adherence to predetermined questions in structured interviews may limit the researcher's ability to access participants and understanding of the research topic (Merriam & Tisdell, 2016).

Semi-structured interviews, which are commonly employed in qualitative research, differ from standardized interviews. According to Doody and Noonan (2013), semi-structured interviews involve the use of predetermined questions, but the researcher has allowed to seek clarification and investigate deeper into the interviewee's responses. This choice is made because semi-structured interviews enable the interviewer to explore the interviewee's comments in greater detail while still adhering to the study's goals (Alshenqeeti, 2014). The other data collection tools mentioned earlier are unsuitable for achieving this specific research objective.

To conduct the semi-structured interviews, an interview guide is created using the research objectives and insights from existing literature. However, due to the flexible nature of the interviews and are open-ended questions which used to explore the issues, making it well-suited for this study (Doody & Noonan, 2013).

Prior to starting the data collection, the researcher obtains ethical clearance from the university, and following the interview guidelines (refers to appendix I) that is data collection permission letter). The interview questions are developed and shared with advisors to check the content relevance of the interview questions and to identify any semantic errors. The interview questions are subjective to achieving the research objectives and addressing the research questions.

During the face-to-face interviews, a total of eight participants are engaged. However, only two respondents are not audio recorded due to their preference and voluntary decision. Before beginning the interviews, the researcher introduces himself to the participants and provided a clear explanation regarding the purpose of the research. It is emphasized that the interview data would solely be used for the current research and would not be shared with any third parties. Additionally, participants are given the opportunity to introduce themselves, highlighting their domain expertise and experiences. Following the introductions, each participant agrees a consent form, which is signed by both the researcher and the participant (that is Participants' Consent Form). The interview sessions lasted approximately 35-50 minutes, during interviewing the researcher takes notes as well as a digital audio recorder to record the discussions.

Semi-structured interviews offer the advantage of allowing the interviewer to investigate deeper by asking additional details information until relevant answers are obtained for the study. This flexibility is one of the strengths of semi-structured interviews in terms of achieving research objectives. Furthermore, the researcher has the freedom to provide explanations or rephrase questions if they are unclear to the respondents. Additionally, the researcher can seek clarification from the participants when their responses are not clear (Doody & Noonan, 2013).

The semi-structured interviews use open-ended questions to gather data, then which are organized into themes and categories. The interview questions are derived from the research problem and are designed to assess the current information security practices in the Ministry of Finance (MoF). These interviews are conducted face-to-face, and the researcher uses a voice recording device, such as a laptop, to capture the audio records of the interviews. Prior to recording, participants provide their consent, ensuring that the interviews are recorded and transcribed for analysis. The interview questions are formulated by reviewing various relevant literature and comment by advisor, which are aligned with the research specific objectives (see appendix II attached for the interview questions).

The evaluation of existing information security frameworks depends heavily on a comprehensive literature review. This involved systematically examining cybersecurity best practices, security policies, procedures, guidelines, and frameworks to gather insights and guidance for the development of an information security framework. Additionally, face-to-face semi-structured interviews were conducted with domain experts from the Ministry of Finance (MoF) to determine

if they had implemented any international cybersecurity standards and frameworks such as ISO 27000 series, NIST Cyber security framework (CSF), COBIT, PCI-DSS etc. These interviews also seek feedback on how these frameworks are customized to meet the specific needs of the MoF. Through this combined approach of literature review and interviews, gaps in the existing frameworks are identified and addressed in the current study.

3.4.1. Data Triangulation

The data gathered through interviews were validated using data triangulation method, which involves the use of multiple methods or data sources to gain a comprehensive understanding of the phenomena being studied. Triangulation is considered a qualitative research strategy that enhances validity by converging information from different sources (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). Different types of triangulations, such as method triangulation, investigator triangulation, theory triangulation, and data source triangulation, can be utilized to strengthen the overall validity and reliability of the research findings.

In this study, data source triangulation was employed to ensure the credibility and internal validity of the research findings. This involved gathering information from a diverse range of domain experts within the Ministry of Finance (MoF) through interviews, document reviews, and observations. By utilizing multiple data sources, the researcher aimed to obtain diverse perspectives and validate the emerging findings. To achieve triangulation, the researcher compared and cross-checked data collected from interviews with correspondents who held different perspectives, thus enhancing the reliability of the data. The three methods used for triangulation in this study are semi-structured interviews, document reviews (specifically analyzing security policies and procedures), and prepared evaluation checklist questions to evaluate the proposed information security framework.

3.5. Research Population

The research population, as defined by Verschuren, Doorewaard, and Mellion (2010), refers to the specific group of individuals that the researcher intends to investigate. In this particular study, the research population consists of domain experts and managers employed in the Ministry of Finance (MoF), specifically selected a sample of 8 respondents out of the total of 12 respondents from the 3 departments of Information Technology within MoF.

3.6 Sample size and Sampling Technique

It is impossible to study the entire population within the Ministry of Finance (MoF), a sample size is chosen to participate in the study. The sample size is determined using a purposive sampling method, which is a commonly used in qualitative research. Purposive sampling allows the researcher to deliberately choose respondents who can provide valuable and in-depth information (Etikan, Musa, & Alkassim, 2016). In this particular study, individuals who possess extensive knowledge and experience in information security are identified and selected as participants.

By using the purposive sampling technique, a total sample size of 9 out of the total number of 3 Technology departments are chosen. The selection of the sample is based on specific IT positions within the Ministry of Finance (MoF), such as Cybersecurity Manager, Cybersecurity Experts, Network Engineers, IT Support, and System Administrators. It is believed that the chosen sample who have comprehensive understanding and awareness of cybersecurity threats and incidents.

To summarize, the purposive sampling technique was employed in this study due to resource limitations, particularly time constraints. Conducting research on the entire population would have been time-consuming and expensive. By selecting a sample, the researcher could allocate resources more efficiently. Additionally, conducting in-depth interviews that taken 40-60 minutes allowed for extracting deep understanding and experiential knowledge from the respondents. This would not have been feasible if the entire population were included. Furthermore, focusing on respondents with extensive experience and intensive knowledge in the domain was preferred over including respondents with limited experience and no expertise, which would have been the case if the entire population were considered.

3.7. Data Analysis

Data analysis involves the consolidation, summarization, grouping, categorization, and reorganization of complex and non-standardized data into meaningful and usable information. Qualitative data analysis encompasses two main methods: thematic analysis and content analysis (Gray, 2014).

Generally, data analysis can be approached in two ways. Inductive analysis involves deriving themes and patterns from the data itself, then which contribute to the development of theory. On

the other hand, deductive analysis starts with pre-existing theories, theoretical frameworks, or hypotheses, and aims to confirm or disprove them through the analysis of the data.

The deductive analysis approach involves researchers starting with a theory to test hypothesis or theory and then confirm or disprove it. This approach is used for positivism research paradigm. On the other hand, the inductive approach involves researchers collecting data with the aim of developing a theory. Unlike deductive analysis, inductive research does not require the creation of a hypothesis. Inductive technique helps researchers to identifying themes or categories from complex raw data, a process known as data reduction. The inductive research approach is typically associated with the interpretivism research paradigm (Saunders et al., 2007).

This study uses an inductive data analysis. According to Saunders et al. (2016), the researcher used inductive analysis method to gain insights into the reasons behind certain phenomena and understand the underlying factors. The research process involves examining information security practices and evaluating the current cybersecurity framework in the Ministry of Finance (MoF). The aim is to assess the level of cyber maturity and identify areas for improvement in the MoF by developing a framework. Gray (2014) notes that qualitative research often utilizes various techniques and approaches to collect data, and it is commonly associated with the use of inductive research design.

According to Wagner et al. (2012, p. 10), one of the main sources of data analysis for qualitative research is the audio and/or video recorded during interviews. The interviews are transcribed from the recorded audio, and the transcripts undergo editing to improve the readability of the transcript while keeping the meaning.

In conclusion, the qualitative data analysis process involves conducting a thematic analysis of the transcribed interviews. In this study, the audio recordings of the interviews serve as the primary data source for analysis. The thematic analysis method is used to identify major themes and categories within the qualitative data.

Data Analysis Process:

Once data has been collected from a selected sample size of population, the next stage is to analyzing the data to address the research questions and objectives. While descriptive analysis is commonly used for qualitative data, the researcher in this study went beyond writing only description by interpreting, understanding and explaining the data. This analysis led to the acquisition of new insights and knowledge. According to De Hoyos and Barnes (2012), state that qualitative data analysis involves the processes of identifying and organizing, coding, conceptualizing, and categorizing themes discovered in the data in order to derive meaning.

Interview data is recorded and then analyzing using a method called coding. Coding involves transforming raw data into a standardized format for analysis (Merriam & Tisdell, 2016). The outcomes of coding are typically referred to as categories or themes, which serve as guiding points for analyzing the data and addressing the research questions and objectives.

This allowed the researcher to develop categories or themes from the data. The researcher repeatedly listened to the interview audio recordings and transcribed the interview content onto the word document. Key points in the transcript were identified then grouped into themes and categories.

By repeatedly listening to the audio recordings of the interviews, the researcher is able to develop categories or themes from the data. The interview content is transcribed onto a word document, and key points within the transcript are identified. These key points are then organized into themes and categories.

3.7.1. Coding and Describing Data

The researcher manually identified themes and categories, which are used as references during the data analysis. Once themes are identified within the transcript text, the analysis process involved data coding. Codes are organized based on their common shared characteristics to create categories and ultimate themes. The coded text is manually sorted to examine the patterns that emerged. The final step required establishing common themes, which directed to the development of a concept represented in the form of a conceptual framework.

3.8. Validity and reliability of the research

Validity and reliability are essential attributes for assessing the quality of research. In qualitative research, terms such as credibility, transferability, and trustworthiness are often used to refer to these attributes (Andrade, 2009).

To ensure the validity and reliability of this research, a triangulated data was used that incorporating multiple data sources from different perspectives. The use of Nvivo software version 10 facilitated data coding and organization (Yin, 2003). While the methodology was thoroughly described to ensure transparency and enable replication of the study. These measures contribute to the assurance of validity and reliability in this research.

Validity refers to the extent to which the research instrument accurately measures what it is intended to measure (Yin, 2003). In this case study, validity is achieved through the use of triangulated data sources and analysis methods, as well as involving key informants in reviewing documents.

External validity refers to the generalizability of research results across different social settings. As this research is a single case study, generalizing to other cases may be challenging. However, single case studies can contribute to theory development and analytical generalization by comparing findings with existing literature. Internal validity relates to the ability of observed variables to predict unobserved variables (Yin, 2003). Themes with higher associations indicate internal validity of the research findings.

Reliability is ensured by providing detailed descriptions of research procedures and standard data collection instruments, allowing other researchers to replicate the study. The researcher used the standard data collection instrument developed for the research (See Appendix II). The use of a digital voice recorder enhances the trustworthiness of the research, reducing errors in note-taking and potential misinterpretation of respondents' views.

Overall, the utilization of triangulated data, used of Nvivo software version 10 for data coding and organizing, and a well-described methodology contributes to the validity and reliability of this research.

3.9. Ethical Considerations

Ethical considerations play a crucial role in the research discipline, particularly keeping human rights and privacy concerns during data collection process. Ethics refers to the principles that command to consider what is right and wrong in research conduct (Muganda, 2010). Even if not explicitly specified, researchers are expected to be knowledgeable (to be aware of) and adhere to acceptable ethical standards in their work.

This study adheres to universally accepted ethical standards, which encompass obtaining informed consent from all participants. Additionally, it addresses important considerations such as voluntary participation, ensuring anonymity and confidentiality, and respecting their willingness. For the respondents given the sensitivity information/data, the researcher explicitly stated that no confidential or sensitive information would be disclosed to third parties or used for other purposes, unless prior permission is granted. Lastly, an ethical clearance was obtained from the AAU Department of Information Science (see appendix I for data collection permission letter).

3.10. Chapter Summary

The chapter discusses the research methodology used in this study. It adopts an interpretive research paradigm and utilizes a qualitative research approach to examine the assumptions of the Ministry of Finance (MoF) regarding information security or cybersecurity practices. The interpretive approach incorporates the triangulation strategy to ensure the validity and reliability of the research being conducted. To determine the study sample size, a purposive sampling technique is employed, specifically targeting domain experts and managers who possess extensive knowledge and expertise in the field. The collection of qualitative data involves conducting semi-structured interviews, reviewing relevant documents, and making observations using a checklist in collaboration with domain experts and managers within the MoF. Each interview is transcribed from the audio recording. Finally, a qualitative thematic data analysis method is applied, whereby data is categorized and organized into themes and categories.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1. Introduction

In this chapter, the result of the collected data through interviews was presented and analysis. Qualitative data for this research study was collected through interviews and observations as well as document review to evaluate current Cybersecurity practices at the Ministry of Finance. Thematic analysis was the chosen method used to review these qualitative data sources. This involved coding the interview transcripts and observation notes to identify common themes, trends and patterns related to Cybersecurity across the Ministry's systems, policies and staff behaviors.

Triangulation refers to the practice of gathering data from multiple sources as a means to establish consistency in research findings. When conducting a study, collecting information from different types of complementary sources allows for cross-verification and corroboration of the evidence. Using interviews, observations, surveys, and documents together allows similarities and differences to emerge that provide a more comprehensive understanding of the phenomenon being studied. The convergence of findings from various data collection methods enhances confidence in the credibility and validity of the results. In this way, triangulation supports more accurate and reliable qualitative assessments.

The proposed framework contains six interacting components that describe the information security practices at Ministry of Finance. These components are: Challenges, Threats, Preventive Mechanisms (Technical, non-technical and Physical & Environmental security, Security Auditing & evaluation and Security Operation Center SOC security monitoring. Each category contains various security domains.

4.2. Challenges

General Concepts:

Challenges refer to the problems, issues, obstacles, barriers or difficulties that an organization faces during implementing, operating, governing, and securing security policies, standard procedures, and a new technological solution. Because implementing and practices of Cybersecurity is always ongoing process with challenges.

Some common potential difficulties an organization has faced or encountered during security practices include Legacy systems that can be challenging to be update, upgrade and secure. For example, older Cisco 2960 switches that are past end-of-life with no more new patches released, Old PCs and laptops may be difficulties to upgrade from Windows 7 to newer Windows 10 and 11. Lack of Cybersecurity professionals and personnel skilled, experienced with complex, newer technologies like SDN technology that has been adopted. Another issue is an insufficient user's awareness training on security policies and lack of general security and inadequate budget and management support for buying network devices and training, and more.

Potential challenges at Ministry of Finance (MoF):

The Ministry of Finance has legacy network devices or older cisco 2960 switches which are past end-of-life (end-of-product, end-of-support) with no more new patches released, which leads to expose security threats and attacks. There is also lack of skilled Cybersecurity expertise personnel. Although somehow awareness training has started giving for managements and experts, not comprehensive to all users. So, there is lack of users' awareness training, this leads non-compliance employees to follow with security policies, rules and procedures while carrying out their daily activities. Even though corporate security policy has been developed and exist, detailed issue specific security policies do not yet cover all l domain services, so far, an issue specific security policy only covering of nine modules of the Integrated Financial Management of Information System (ISMIS) one department.

Researcher believes there is lack of commitment from employees to adhere to security policies, rules, procedures and guidelines during their regular work (while they are carrying out their daily tasks). This non-compliance comes from a lack of knowledge, understanding, comprehensive awareness training that has not been not given or provided to all employees. The Ministry of Finance has not enough qualified Cybersecurity experts and skilled staff. With nowadays, cyberattack has become rapidly growing more sophisticated (complex and dynamic) due to leveraging is machine learning and AI, so proactive defense requires skilled and specialized Cybersecurity professionals who deeply familiar with advanced on technological safeguards.

According to Respondent 1 said that:

> *" There is a lack of comprehensive awareness training provided to all users and employees covering the details of developed corporate security policies, issue-specific policies, rules,*

procedures, and guidelines. And general security training is also insufficiently offered across the organization's employees. ‘‘

The respondent tried to disclose that, the lack of security-oriented mindsets and culture is driving non-adherence within the organization. work habits and priorities that do not account for security needs also contribute to this non-compliance.

Another Respondent 2 described that non-compliance with security policies, rules and procedures stems largely from resistance to adapting workflows for new technologies and policies. Most employees remain focused only on completing tasks and reporting as usual, without integrating a security mindset into their regular work. There is an organizational culture gap in grasping security's importance alongside simply finishing assignments in customary fashion.

Another significant issue is the lack of commitment and dedication from employees to adhere to organizational security policies and procedures. There is also unwillingness toward adapting and adopting new technology solutions and technological changes. Additionally, there is a shortage of professional Cybersecurity experts within the organization.

In conclusion, deficiencies exist in employee knowledge of, commitment and dedication to security policies, rules, procedures and guidelines. There are also gaps in understanding and utilizing technological solutions like antivirus, firewall, web application firewall, domain controller, network access control. These shortcomings drive resistance to complying with new security policies. Fill the gap by awareness training, change security mindset and culture in organization efforts and skill building are required.

A significant concern raised by the majority of respondents was the vulnerability of financial institution, particularly MoF, to phishing and social engineering attacks. Phishing involves the deceptive impersonation of trustworthy individuals to gain access to sensitive information like usernames and passwords. Hackers are increasingly sophisticated in their tactics, using fraudulent links and dangerous email attachments. Therefore, enhancing security awareness is crucial for the safety of financial institutions, especially those providing digital finance services, with MoF being one such institution in the offering of the digital services sector.

Findings, the key challenges identified within MoF include a lack of comprehensive training to increase user awareness about security policies, gaps in technical skills, and a shortage of certified

cybersecurity professionals who can effectively navigate the rapidly evolving landscape of emerging technologies and implement new attack and prevention mechanisms. Non-compliance among users due to a lack of awareness and resistance to adopting and adapting to new technologies. Many ordinary users have lack of adapting a new technology, resulting in negligence towards security policies and standard procedures.

4.3. Threats

General concepts or idea about threats:

A threat refers to a potential danger that can exploit vulnerabilities and cause harm. It can be either physical or digital in nature. Physical threats involve tangible risks that compromise physical assets and infrastructure, such as theft, fires, water leaks, and equipment failure. On the other hand, digital or cyber threats target computing systems, networks, devices, and digital infrastructure to disrupt operations, gain unauthorized access, or steal data.

Common categories of cyber threats include malware, which encompasses various forms of malicious software like viruses, worms, spyware, adware, Trojans, ransomware, and botnets designed to infect systems and damage files. External threats are typically known as those originating from outside corporate networks, such as phishing emails that deceive users into revealing passwords or sensitive information, denial-of-service (DoS) attacks that flood systems with excessive traffic to overwhelm capacity and crash services, data breaches involving the theft and exposure of confidential information, brute force attacks where hackers attempt to guess weak login credentials, and zero-day threats, which are complex and unrevealed flaws that have no patches yet.

Internal threats, on the other hand, involve data theft, fraud, or sabotage by employees who abuse their system access privileges. These threats originate from within the organization's internal networks.

To protect the confidentiality, integrity, and availability (CIA) of critical infrastructure and sensitive information, it is crucial to design and implement tailored multiple layered controls. These controls can be technical (such as multi-factor authentication, strong password policies, firewalls, intrusion prevention systems, software updates, antivirus, bring your own devices security protection (network access control, NAC technology), backup and recovery services),

non-technical (including administrative measures, policies, and awareness training), and physical measures (such as CCTV security camera, fire alarm systems, access control system with combination of finger print plus PIN plus card). By implementing robust security countermeasures, organizations can mitigate the risks posed by various threats and ensure the protection of their assets and information.

Threats at Ministry of Finance (MoF):

As a financial institution, the Ministry of Finance (**MoF**) faces threats for the purpose of illegitimate financial gain from both internal and external sources. These threats manifest in digital/Cyber forms as well as physical attacks. Common Cyber threats include various types of malwares (viruses, worms, Trojans, ransomware), social engineering tactics such as phishing emails, sniffing to intercept network traffic (also called man-in-the-middle attacks), denial of service (DoS) attacks, fraud, unauthorized remote access, and data leakage or theft. Physical threats also present risks to the integrity, confidentiality and availability of the Ministry's systems and assets through means such as unauthorized building access or theft of devices and records. Defending against this diverse array of Cyber and physical threats from both insiders and external actors remains an ongoing challenge to secure the Ministry's operations and sensitive financial resources in the face of motivated criminal or attackers. So, implementing robust information security controls and staff training serves as a necessary to countermeasure.

The Ministry of Finance has experienced various physical security and Cybersecurity threats, as learned from interviews with employees in different roles. To minimize insider risks from potential employee mistakes that could unintentionally compromise security, the Cyber Security Unit department continuously conducts security awareness training. All interview respondents agreed that they did not believe any employee would intentionally pose a threat. Currently known Cyber threats include malware like viruses, worms, Trojan horses, botnets, ransomware, phishing emails, denial of service attacks, social engineering, fraud, and remote access threats that can lead to data theft and leaks. Physical security threats have also materialized such as unlocked floor racks, material theft, weak device passwords, writing down passwords, and password sharing among colleagues.

According to Respondent 1 said that:

> *"The Ministry of Finance faces both physical and Cybersecurity threats. He outlined some of the array of Cyber threats, including computer viruses, worms, Trojans, ransomware, and other types of malwares like botnets. Phishing attacks, denial of service (DOS) attacks, and variety forms of social engineering tactics (for example, asking questions like: where are you doing? What do you do? What kind of service your organizations offers? what kind of technological control or countermeasure used?) such kind of questions I am asked several times from different persons at the time of I participated to Cyber Security workshop training, I thought* these are considered as Cyber threats for MoF. A specific example of a Cyber incident was happened before, as respondent 1 expressed, once up on a time a lot of employees had received a bulky email message which is phishing attack. "

Another Respondent 2 shared his belief that any device connected to the corporate network poses a potential security threat unless its defenses are verified ahead of granting access or assured the compliance of security posture. He reasoned that all lived on the uncertainty of Cyber/digital space which means the one's cannot be assumed his device is secured. As a example, Respondent 2 admitted sometimes he used his flash disk without scanning it for malware first, even though he has Avast antivirus installed due to time-consuming nature of scanning large files within flash drives has led him to insert drives urgently without scanning. For some reasons, he has disabled his Windows personal firewall and forgotten to re-enable it (turn it back on) before accessing the internet. With the firewall disabled, his computer loses that layer of protection and becomes exposed to greater Cybersecurity vulnerabilities from online threats.

As Respondent 2 stated that:

> *"We have network devices in use that are already past their* ***end-of-life*** *date. Which means the products are no longer being sold, manufactured, or supported by the vendor (that is end of product, end of sell & end of support date). These network devices which are entered end of life date, pose a security risk and take them as security threat since they can no longer receive updates of security patches to fix vulnerabilities."*

Researcher thinks and believes that everyone who is workforce of MoF must follow and read predefined security policies, standard procedures and guidelines if there is time constraint and urgency, they can ask their senior for further support.

The respondent 3 raised the point that:

> *"Information technology and technical tools are like a two-sided coin. on one side they provide protections, but on the other side they may be enabled threats/vulnerabilities. As we are technology early adopter, we don't know what is going on at the background (there may be backdoor) unless we verify it by our own skill."*

According to researcher noticed during interview conversation with respondents, researcher believes that the Cybersecurity threats described by Ministry of Finance respondents in various roles are there. In addition to respondents mentioned, there is also keylogger attack which should be taken as threat. A keylogger attack is a common technique used by hackers to steal sensitive information like credentials. It involves the hidden remote installation of malicious software or hardware that secretly records a user's keyboard input without their knowledge. The keylogger captures sensitive information entered by the user such as login credentials and passwords. The attacker can then access this collected data to illegally gain access to private accounts and sensitive systems. This malicious software can be secretly installed when users download legitimate-looking software that has a hidden dual-agent keylogger component. Once this malicious software is installed on a user's device like a laptop, PC, smartphone or tablet, the keylogger records and sends all keyboard input to the hacker. I recommended preventative controls include antivirus software, safe web browsing, multi-factor authentication, and aggressively giving Cybersecurity awareness training to employees to mitigate this threat in addition to technological solutions to control preventive mechanism.

Over the last 10 decades, Cybercrime has become a severe and widespread threat that impacts all governmental and non-governmental organizations. Thus, organizations must build a shared Cybersecurity culture across their employees or workforces and proactively against Cyber threats in advancing. This includes aggressively conducting continuous security awareness training programs to educate their employees; Implementing robust technical controls and keeping them updated. Ultimately, organizations need to make Cybersecurity a priority if they are to have any hope of getting ahead of the threats instead of always reacting to the latest attacks. Comprehensive preparation and dedicated resources are vital to increase Cyber resilience in the face of the growing sophistication of Cyber criminals. No single solution will provide a silver bullet, rather an array of sustained efforts are required to mitigate risks posed by Cyber threats in the years ahead.

Findings, the main threats faced by the MoF as a vulnerable financial institution were identified the various forms of malware such as viruses, Trojans, worms, ransomware, DOS/DDOS attacks, bot/botnets, keyloggers, and social engineering techniques like phishing attacks through email, fraud, data thefts, data deletion, sniffing, and man-in-the-middle attacks.

4.4. Facilitating conditions

General concepts:

Facilitating conditions for effective information security preventive mechanisms require senior & top management support, commitment & dedication give time and efforts to promote security culture; adequate budget and resource allocation for modern security technologies/controls and enforcement; accountability for non-compliant users with security policies; user awareness and training programs; and a dedicated Cybersecurity unit responsible for security posture auditing and monitoring. Additionally, corporate security policies should follow and align with national Cybersecurity policies without any contradiction.

Facilitating conditions at Ministry of Finance:

The leadership and top/senior management are supportive, committed & dedicated to Cybersecurity by allocating sufficient budget to establish a Cybersecurity unit and ensure compliance. They invest time and effort, encourage to develop Minster of Finance security policies and Cybersecurity framework that align with national Cybersecurity policies. Before a dedicated Cybersecurity Unit is being established, the governance and accountability around security issues lies fragmented across various financial systems and software development departments. There is no centralized ownership to comprehensively manage vulnerabilities and threats.

As researcher, in my opinion, I understood and observed that support from top and senior management and leadership is good. For example, to be created a dedicated Cybersecurity Unit or department and allocating sufficient budget to upgrade network infrastructure and security project. This includes purchasing new network devices, deploying projects to build modern infrastructure like software-defined networking in data centers, implementing advanced firewalls, network access control systems, etc. For reference, I reviewed well-defined corporate and issue specific security policies that aligned from national security policy. Overall, top managements are dedicated and committed by supporting budget for awareness training to reach to every employee.

For example, they rent a training room at, 5killo university, I confirmed by went there and participated while giving awareness training. They have training schedule every week morning from 8:30 up to 9:30 AM. Their willingness to facilitate conditions and provide financial support enables to develop security systems and policies.

Respondent 1 said that:

> *"Before the establishment of a dedicated Cybersecurity unit, Cybersecurity issues and responsibilities were dispersed across different departments. For instance, the nine modules within the Integrated Financial Management Information System (IFMIS) were each administered by separate teams that managed Cybersecurity only for their own services, rather than having centralized governance. However, as respondent 1 highlighted, top and senior managements have a good willingness and awareness regarding Cybersecurity matters. This commitment has enabled the creation of a dedicated Cybersecurity Unit that can now centrally manage and govern the Cybersecurity vulnerabilities, threats and be accountable for safeguarding the system."*

As a researcher, I have observed that the Cybersecurity Unit operates as a dedicated directorate-level office. Within this unit, there are three specialized teams such as the Cybersecurity Engineering Team, the Cybersecurity Operations Team, and the Cybersecurity Policy and Governance Team. Each team plays differentiated roles and responsibilities that have been delegated to them in order to comprehensively administer Cybersecurity matters. This structure allows to efforts while retaining centralized governance under the Cybersecurity Unit.

According to another respondent 2 stated that:

> *"The top managements have a strong commitment and dedication to supporting the Cybersecurity Unit. For instance, after established Cybersecurity Unit structure, Unit wrote three major project proposals, first proposal is developing Cybersecurity policies with alignment to national Cybersecurity policy, second proposal is upgrading the data center's network infrastructure and security controls mechanisms with modern technologies, and third proposal is renting dedicated offering awareness training room at the 5killo University campus. All these three project proposals were presented to the top and senior managements with justifications for why the investments were necessary. Then the top managements approved and allowed the budget for all three project proposals submitted by the*

Cybersecurity Unit. These is shown the top managements have commitment and dedication, willingness and support to prioritize Cybersecurity."

In conclusion, there are various facilitating conditions that empower the Cybersecurity Unit to effectively carry out its critical mission. These enabling factors include ongoing support from top management through budget allocations for procurement security devices, implementing safeguards, and conducting awareness training. Additionally, the creation of a dedicated Cybersecurity Unit that focused only on digital defense of security. Finally, the development of national Cybersecurity policies provides a crucial framework to guide and to develop the Cybersecurity Unit's security policies and strategical, tactical and operational techniques. Together, these facilitators with a strong commitment and dedication of across top managements support, security policy makers and technical security implementers empower to growth Cybersecurity Unit.

Findings, the other findings that identified during interviews was the positive endorsement from top and senior management regarding budget allocation for the procurement of devices, software, licenses, and the upgrading of network infrastructure, as well as for technical training and workshops. The creation of a dedicated Cybersecurity unit, with accountability and responsibility, emerged as a powerful measure to enhance the prevention and improvement of Cybersecurity attacks.

4.5. Preventive Mechanisms (PM)

4.5.1. Technological enforcement solutions (Technical PM)

Overview:

Technological solutions in the context of information security practices refer to the various hardware and software systems, tools, and controls that are implemented to protect an organization's data, infrastructure, and technology assets.

Some of the key technological solutions implemented by organizations for information security practices include next generation firewalls, endpoint security protection for Bring Your Own Device (BYOD), network access control (NAC) technology, antivirus software, active directory/domain controller (AD/DC), web application firewalls (WAF), SDN technology for data center networking and infrastructure, load balancers, and backup/recovery capabilities at remote

disaster recovery sites. These solutions provide crucial safeguards for securing networks, devices, critical systems, data and applications through advanced threat protection, identity and access management, network segmentation, availability assurance etc. Adoption of such robust security technologies is vital for organizations to strengthen their security posture.

The goals of these technological solutions are to safeguard confidentiality, integrity, and availability of information by preventing, detecting, and responding to Cybersecurity threats and vulnerabilities. Effective solutions take a layered defense-in-depth approach to provide controls to secure overall organizations information systems resources such as network infrastructure, endpoints, applications software, valuable information/data assets and technology itself.

Various Technological solutions at Ministry of Finance:

General Concept/idea of Next Generation Firewall (NGFW):

Firewalls are critical network security devices, which are either hardware, software, or both, that filter incoming traffic that come from untrusted network (internet) to internal corporate networks, and outgoing traffic from corporate networks to the internet. Firewalls can be placed internally or at network perimeters.

Next-generation firewalls (NGFWs) re advanced network security devices that go beyond traditional firewall capabilities by integrating advanced capabilities like deep packet inspection, real-time malware analysis to identify viruses, spyware and threats, and machine learning for dynamic and adaptive protection. NGFWs provide comprehensive inspection of all network traffic. NGFW is deployed with single failure redundancy for both Internal and external firewalls to eliminate any single point of failure availability. But previous early used legacy firewall had lack of redundancy.

As researcher, from my assessment, the Ministry of Finance has deployed and implemented Palo Alto's next-generation firewall solution, which utilizes machine learning to enable dynamic and adaptive threat protection. This advanced system comes with several feature capabilities like antivirus, data loss prevention (DLP), deep packet inspection for detailed traffic analysis, and real-time malware detection, spyware, web filtering, and other threats.

According respondent 1 stated that"

> *"A machine learning-driven next generation firewall (PaloAlto brand) has been deployed and implemented with redundancy or failover in Minster of Finance to filtering and protecting incoming traffic from untrusted network (Internet) into our trusted internal corporate network and vice versal. According to another respondent, the Palo Alto firewall that is deployed and implemented in addition to core security functionality, but it also supports remote access VPN capabilities. This allows IT support staff and software developers at the Ministry of Finance to securely work remotely when necessary. Previously, remote work solutions like AnyDesk and TeamViewer were used to facilitate remote work, but these carried built-in security risks and vulnerabilities."*

From my observation, the Palo Alto firewall solution offers various built-in security capabilities as part of its overall product portfolio, including intrusion prevention system (IPS), data loss protection (DLP), antivirus, DNS security, web url filtering features and advanced threat and zero-day attack etc. The only things that are required purchasing the required licenses and configuring it as needed.

In the absence of a commercial license, a product may only provide basic feature support, meaning it functions as required but lacks additional capabilities. Nowadays, vendors offer security products as a portfolio, integrating all features into a single hardware device rather than using separate hardware modules as in the past. This provides the advantage of purchasing a device and later activating specific features by simply purchasing the required license.

General Concept/idea of Web application firewall (WAF):

A web application firewall is a security solution that designed to monitors, filters and blocks harmful malicious traffic directed or targeted to web applications. It inspects web requests in order to detect common attack methods such as SQL injection. On top of analyzing the contents of web traffic, the primary function of a WAF is to filter and safeguard URLs and domains.

Web application firewall at Ministry of Finance:

The Ministry of Finance has deployed a robust, enterprise level web application firewall (WAF) solution to filter and safeguard their URLs, domains and prevent application and database level attacks like SSQL injection. All incoming and outgoing web traffic is routed through the WAF,

which examines the traffic. Previously, a basic proxy server was utilized, rather than a full-fledged web application firewall.

Based on my observations, the Web Application Firewall (WAF) at the Ministry of Finance has been set up and configured to filter content level. Specifically, the WAF blocks access to unwanted sites such as torrents, as well as social media platforms like Facebook, Telegram, TikTok, YouTube etc. Currently, with the next generation firewall operating at the application layer 7 of the OSI model, it is capable of filtering and blocking content level, similar to a Web Application Firewall (WAF). As a result, security vendors are attempting to integrate WAF functionality into next generation firewalls to eliminate redundancy and reduce the need for separate hardware purchases. This consolidation aims to modernize security measures and minimize costs associated with hardware acquisition.

As explained by Respondent 1:

> *"Our financial institution provides over 90% of public services through online internet access; our web applications are the most vulnerable attack surface for hackers. So, to protect these critical web application systems, we have developed a WAF security layer as an additional line of defense."*

Web application firewall functions as a proxy server that was utilizing at past legacy solutions for traffic filtering and caching. When searching for information on Google, the traffic gets routed through the web application firewall.

Respondent 2 described that web application firewalls have become one of the most valuable security tools. Today's web application firewall solutions utilize advanced analytics like machine learning and behavior analysis to provide robust protection and greater visibility. Respondent 2 clearly believes web application firewalls are filtering, monitoring, and preventing access to malicious URLs and domains when searching for information on the Internet.

Respondent 3 stated that:

> *"Our current F5 WAF appliance safeguards against DOS, DDOS, botnet attacks, fraud, URLs, domains and the top 10 Open Web Application Security Project (OWASP) threats. However, a traditional proxy server was limited in its capability, only providing web traffic filtering and blocking access to undesirable websites, without protection against Cyber-attacks."*

General Concept/idea of Antivirus:

Antivirus software is a program designed to detect, block, and remove viruses and other kinds of malicious software like spyware, ransomware, and Trojans from a computer. It works by scanning files, memory, and disks to look for virus signatures and behaviors that suggest an infection. Quality antivirus software runs automatically in the background to provide real-time protection.

A virus definition is a set of signatures or patterns that antivirus software uses to detect specific malware, viruses, and other threats. Maintaining up-to-date antivirus virus definition, it protects computers and systems from the latest malware zero-day attacks.

Antivirus at Ministry of Finance (MoF):

At the Ministry of Finance, they have deployed Symantec Endpoint Protection licensed server based to centrally manage antivirus protection across their systems. This is enterprise level antivirus solution, which requires a paid license, enables automatic updates of virus definitions from the Symantec cloud server and then from local Symantec antivirus server push virus definition updates to endpoint clients based on configured schedule. This antivirus software detects and identifies malware, ransomware, and other Cyber threats before they can compromise their systems and data. This prevents breaches, data leaks, corruption and theft that could occur if an infection was allowed to propagate. Additionally, Symantec can detect risky email links and attachments before users open them.

Based on my evaluation, I observed some good security practices in place. For instance, they utilize a purchased Symantec endpoint protection solution, which offers more security capabilities than just using Symantec antivirus software, which has its limitations. Another positive quality is that they transitioned from using a free antivirus to a commercial antivirus solution. This likely provides them to better secure their systems and data. Overall, the use of enterprise-level endpoint protection as well as stopping free antivirus, it shows their security consciousness.

Respondent 1 said that:

> *"Previously, employees used various standalone free antivirus programs such as Smadav, Avast, Kaspersky, McAfee, Avira, Norton, Windows Defender, 360 Total Security etc. They download directly from Internet and install and use it to prevent common virus but not latest malware zero day attacks. However, after joining the computers to the domain controller, the*

organization purchased the enterprise-level Symantec Endpoint Protection server based solution. This centrally pushes virus definition updates from a local Symantec manager rather than individual vendor cloud servers, this improving system performance and protection. The licensed Symantec antivirus has several key security features and advantages, including data loss prevention, zero-day attack blocking, memory vulnerability defense, and protection against viruses, worms, ransomware, and other malware types."

Respondent 1 described also his experience, viruses and malware that enter through external devices like external hard drives, flash drives, memory cards, etc. can be better prevented by using an up-to-date licensed antivirus solution instead of a free antivirus.

Respondent 2 explained that:

"Early years ago, when employees individually had downloaded and installed free antivirus software; It was up to each user to manually initiate scans of external devices such as flash drives, which wasn't mandatory. This approach posed a risk of malware entry if users neglected to scan external media that is open files directly without scanning flash disk. However, today after users are joined into a domain controller, Symantec Endpoint Protection, the antivirus management server enforces users to scan his external devices like flash drives before access. As a result, users experience a delay while large files are scanned, which can slow down performance due to the real-time scanning of external media. Virus definition updates are now centrally managed, with the central antivirus server receiving updates from the vendor's cloud and then distributing them to client computers, rather than each client updating individually."

In my perspective as researcher, I believe that antivirus software is one layer of protection of security, but not yet it against all threats entering through the Internet or external devices such as USB drives. For users of Windows, it's crucial to maintain the Windows Defender Firewall always make active for both private and public networks. It's strongly recommended not to be disabling or turn off this firewall, as considering a multi-layered defense strategy.

Respondent 3 strongly emphasized that:

"The fact that while the Ministry of Finance has implemented the purchased licensed Symantec Endpoint Protection antivirus for users and systems connected to the domain

controller, there are exceptional certain system users who are not use this Symantec antivirus due to lack of domain member, they continue to use free antivirus solutions like Avast, alongside the Windows Defender Firewall. Additionally, guest users and partners who use their personal laptops often rely on free antivirus software. These users, who do not utilize the licensed enterprise-level Symantec antivirus, potentially expose to security vulnerabilities."

As a researcher, I recommend to all employees, whether they are system users or regular internet users, is to use at least a standalone commercial antivirus program if they are unable to connect to a domain controller with different reasons. This is because security vulnerabilities can arise from minor issues, not just big ones. It's important to have a reliable antivirus solution to provide a basic level of protection against these potential threats.

General concept/idea of Active Directory/Domain Controller (AD/DC):

Active Directory is a directory service that stores and organizes network objects or resources in a hierarchical manner, whereas a Domain Controller is a server that manages and authenticates network access for domain users. Domain controller is central management of user accounts, security groups, computer resources, and other network objects. Both services are developed by Microsoft and exist within windows domain environment. Domain is collection of objects like users, groups, computers, printers etc. under the management of domain controller.

Active Directory and Domain Controller at Ministry of Finance:

The Ministry of Finance has implemented a robust Active Directory/Domain Controller system with redundancy to ensure high availability. This centralized system enables creating and pushing policies to all user computers on the domain. Now, domain-joined users cannot freely install software on their computers without intervention from IT administrators. This restricts software installation rights as a security measure. Previously, users could download and install programs, some of which might have contained exploits or malware if they came from untrustworthy sources. By locking down software controls, the risk of attackers compromising systems via malware payloads is greatly reduced. The Domain Controller acts as an additional layer of protection by preventing unauthorized software installation across the ministry's technology infrastructure.

The researcher point of view, the AD/DC acts as the central repository for all user accounts and credentials across the ministry's networks. The AD/DC is like gatekeeper, ensuring only authorized

users can access confidential information like budgets, payroll, load data etc. Several policies configured for different domain users for example, configure the same desktop settings for all users, restrict software/hardware installation, define password complexity rules and so on.

As respondent 1 said that:

> *"Above 1,000 users or computers have been joined into the domain controller to enforce various policies from central. As a result of this policy, end users are no longer able to install software on their own without IT administrators. Instead, if a domain user wants to install new software, they must submit a request to the IT technical support team. Then IT administrators install the software on the user's computer."*

The researcher explained that the domain controller centrally enforces and authenticates various policies on domain-joined user computers. This centralized management of user devices joined to the domain controller makes it easy to administer and control end user machines by enforcement policies centrally. Specifically, the domain controller enables single sign-on access and permissions to corporate resources across managed computers.

The respondent 3 explained that:

> *"All users log into their computers using domain-joined accounts rather than standalone local computer accounts. This means that the user accounts and credentials are centrally managed through the domain controller. If a domain user forgets their login password, they can contact the system administrators for assistance. The user would inform the administrator that they are unable to access their computer due to a forgotten password. The administrator can then reset the password on the domain controller, setting a default temporary password such as "P@$$w0rd" for the user. Additionally, the administrator enables a rule forcing the user to change the password upon their next login."*

According to the researcher's view, the domain controller's centralized management of user credentials allows IT administrators to easily reset forgotten passwords for domain users. By enforcing a password change after resetting a temporary password, it ensures users will choose a new password of their own, rather than continue using the temporary password they've been assigned. This maintains better security. Additionally, having domain-based user accounts provides manage and control of credentials as compared to standalone, that is locally-managed

accounts. The domain system gives administrators accountability over user access across all connected devices.

In summary, domain controller serves a number of purposes, such as distributing updated virus definitions to all domain-connected user devices. They also allow centralized control and prevention of end users installing unauthorized, illegal or unknown applications software that could pose security risks if left unmanaged. Moreover, domain controllers enable blocking the use of flash drives through centrally applied policy enforcement.

However, there are some limitations with the domain controller system. Users/employees who do not join their devices to the domain remain outside the control of its security policies. Additionally, guest endpoints that temporarily access the corporate network cannot be governed to the same extent as domain-joined computers.

General idea of Bring Your Own Device Security Protection (BYOD) using NAC technology:

Network Access Control (NAC) technology serves as a security measure for managing the risks associated with Bring Your Own Device (BYOD) policies. NAC solutions enforce security policies by assessing devices for compliance with established security standards before allowing them to connect to the network. Devices that don't meet the necessary security policies such as smartphones, tablets, and laptops, can be quarantined or given limited access via separate virtual LANs to prevent them from reaching critical information systems. Every time when a new endpoint tries to connect to corporate networks, NAC device assess device’s security postures.

NAC solutions can identify and evaluate devices as soon as they try to connect, checking for up-to-date antivirus software, appropriate system updates, and other security configurations. If a device fails to meet the criteria, NAC can deny network access, place the device in a quarantined area, or provide limited access to computing resources. This helps to prevent potentially vulnerable or compromised devices from accessing sensitive areas of the network, thereby protecting against unauthorized access and Cyber threats.

In conclusion, non-compliant personal devices like smart phone, tablet and laptop can be isolated or restricted through segmented virtual LANs preventing access to sensitive corporate information systems.

BYOD Security Protection at Ministry of Finance:

The Ministry of Finance has implemented ForeScout's NAC technology to enhance the security management of BYOD practices. This technology is particularly aimed at safeguarding personal devices such as laptops, smartphones, and tablets that are not managed through a domain controller. These endpoints are potentially vulnerable and at risk of Cyber threats due to outdated antivirus programs, missing security patches, obsolete operating systems, and the presence of malicious applications, all of which can create openings for Cyber attackers to exploit.

Previously, the Ministry of Finance lacked control mechanisms for endpoint devices, particularly those belonging to guests and partners, despite having a licensed Symantec Endpoint Protection antivirus for employees who are joined to the domain controller. The MoF is utilizing a network access control (NAC) solution for the first time to control and manage endpoint devices.

Based on my observations, it is highly advisable to utilize a network access control (NAC) solution to manage and secure not only the organization's own computers and laptops but also the personal devices of guests and partners. The Ministry of Finance has adopted ForeScout's NAC technology, which offers support for centralized account management using AAA protocols such as TACACS+ or RADIUS, even it is used for legacy network devices. This implementation enhances the security posture by ensuring that all devices, regardless of ownership, are subject to rigorous access controls and policy enforcement when connecting to the network.

Respondent 1 described that:

> *"The use and effectiveness of a network access control (NAC) solution in managing endpoint security, particularly for personal devices as internal users or employees and guest & partner. For example, a technician utilizing their own laptop might it be compromised with malware or hacker's keylogging software. A NAC solution is identifying and controlling endpoint devices, ensuring they meet security standards before granting them entry to the corporate network, thus mitigating potential threats."*

Respondent 1 clearly defined that NAC gives us visibility into any endpoint device trying to connect, NAC will check if the latest patches are installed, antivirus with latest update is installed, personal windows firewall is on, and other security controls meet our policies. If not, we can

restrict access or route them into a separated network with isolated pr-prepared VLAN with limited access to protect our core infrastructure until the device is compliant.

In my opinion (researcher), I believe that implementing a NAC solution is an effective preventive strategy. It audits the security status of any endpoint devices attempt to connect to the Ministry of Finance's network. The NAC checks for up-to-date security patches, active antivirus programs, and enabled personal windows firewalls etc. Endpoint device which si not compliant with the predefined security requirements or policies, it can be either provided a limited network access or directed to a specific isolated VLAN. This partitioned network is designed with limited permissions to protect the core infrastructure until the endpoint complies with the required security policies and standards.

Another respondent 3 described that*:*

> *"NAC solutions are used for dual purpose, primary enforcing BYOD security policies, secondly for the centralized management and configuration of network devices using TACACS+ or RADIUS protocol servers for authentication, authorization, and accounting (AAA) to secure network device accounts. However, older personal devices not compatible with Windows 10 or newer versions may face limitations when connecting to the corporate network. These devices might be restricted to only accessing the internet and not be permitted to reach the company's information system resources. This security measurements ensures that outdated technologies, which often lack the latest security features and updates, do not access corporate Information systems."*

In summary, implementing a Network Access Control (NAC) solution is crucial for effectively managing and preventing security threats from endpoints, particularly when guest and partner devices attempt to access the corporate network and information systems resources of MoF. Since these devices have not been integrated into MoF's domain controller, they are assigned to the guest WiFi network, which restricts their access to the Internet only.

General concept/idea of Software Defined Network (SDN) technology

Software-defined networking (SDN) refers to a new paradigm or modern network architecture for managing and configuring data center networks. It is automated and centrally network policies enforcement. The main advantages/benefits of SDN over traditional network architecture is its

agility and flexibility. it distinguishes or separates the control plane, data plane and management plane, which is putted all-in the one in the traditional network architecture. The SDN's architecture, which uses spine-leaf and Application Policy Infrastructure Controller (APIC) topology that connected via layer 3 or IP-based communication, due to this reason, it provides several benefits. It allows high-speed connectivity that operate at full speed of device's interfaces or ports. Therefore, there is advantage of gaining high speed that is device's interface/port speed as it is and loop free at all.

Software Defined Network (SDN) at Ministry of Finance:

The Ministry of Finance has implemented a new, modern paradigm center network infrastructure for their data center. By implementing Software-Defined Networking (SDN), they have gained several advantages, including enhanced security and performance. This is achieved through the segregation of policy management, data forwarding (data plane), and route decision making (control plane), which allows for more efficient and effective management of network policies and resources.

Respondent 1 explained that:

> *"In 2023, our data center network infrastructure is upgraded with the adoption of SDN technology. This replaced our previous traditional network architecture (three/two layers such as Access switch, distribution switch and core switch or access switch & collapsed core switch). The SDN solutions provides the management and enforcement of network policies."*

In my point of view as a researcher, I believe that SDN solutions are well suited for complex environments that massive traffic volumes and complex configuration. However, specialized skills are required to properly implement, operate, and maintain an SDN deployment. The redundancy and high-availability built into SDN architecture help mitigate the risk of the potential of hardware and software failures and faults.

The main challenges are the technological skill gaps required for implementation and ongoing maintenance. When failures do occur, highly trained and skilled staff are crucial to resolve issues and minimize downtime. Overcoming these knowledge gaps across IT teams is essential for realizing the benefits of SDN and ensuring continuous delivery of mission-critical network services. the mean time to overcome these challenges.

Respondent 2 raised that:

> *"The significant limitations in our traditional network setup, specifically the presence of single points of failure due to on a single core switch and a single firewall. This data center is suffered from a lack of redundancy, in case the network faults is encountered a problem, then immediately service is interrupted. So, with the adoption of a contemporary software-defined networking (SDN) architecture, enhanced our data center infrastructure's. By implementing pairs of core switches and firewalls redundancy, it is enhancing fault tolerance and minimizing the risk of downtime due to hardware failures or maintenance."*

General concept/idea of Load Balancers:

Load balancers distribute workloads across multiple servers, ensuring no one server is overwhelmed. This improves application availability and performance. The load balancer acts as a reverse proxy, receiving requests from clients and forwarding them to the appropriate server resource based on load, response times etc. Load balancers provide a critical role in sharing workloads efficiently across available compute resources to avoid bottlenecks and enhance performance.

Load balancers at Ministry of Finance:

The Ministry of Finance has deployed redundant F5 load balancers in their data center to distribute incoming traffic across their servers. By load balancing requests across multiple servers based on availability and workload, the F5 implementation is able to improve response times for users. The traffic is automatically directed to servers with free or low workloads servers, increasing overall speed and performance. The redundant F5 devices ensure continuity of services if one load balancer fails, it works with second load balancer. In this way, the Finance Ministry aims to provide reliable and quick access to their applications and resources through effective use of load balancing technology.

Before implementing the F5 load balancers, the application servers were heavily burdened with congested traffic bottlenecks. With no effective traffic distribution method in place, requests flooded into servers without accounting for their current workload and availability. This created for degrading performance for users. The lack of load balancing resulted in an uneven traffic distribution and failure to leverage unused resources optimally across the infrastructure.

According to researcher view's, the main advantage of load balancers with redundancy is gaining **availability**, **performance** and **security issues**.

As respondent 1 described that:

> *"The Ministry of Finance recently (in this 2023 year) has implemented redundant F5 load balancers to better distribute traffic across backend servers. These load balancers manage workloads by routing requests to available systems that have low workloads. The redundant configuration also provides fault tolerance if the primary load balancer experiences hardware failure, goes down or other issues, the secondary load balancer can seamlessly take over traffic distribution. In this way ensure business continuity without service dropping out. This is high availability design that delivers seamless failover as well as effective workload or traffic management to optimize resource usage."*

As respondent 1 said, deploying redundant load balancers avoid network traffic congestion and bottlenecks, it assures availability and performance.

Researcher confirmed that the Ministry of Finance serves numerous customers, including government organizations and registered traders who access their digital finance services and engage in online transactions. To improve performance, minimize bottlenecks, and reduce network congestion, implementing a load balancer is a viable solution. This ensures that network traffic is distributed efficiently across multiple servers, optimizing resource utilization and enhancing overall system performance.

General concept/idea of Backup and Recovery services:

Backup refers to creating copies of data or system configuration (clone) into separate dedicated disaster recovery site storage servers' system and snapshot volumes to enable recovery or restoration in case of data loss due to several reasons such as system failure, deletion, Cyber-attacks, or other issues. Common backup types are full, incremental, differential. Backups can be stored on physical media (tape recorders) or in the cloud servers. Backup schedules is the frequency and intervals in which backups run. **Recovery** is the process of restoring backed up data or systems after data loss or failure events. This allows restoration of systems to a last known good state.

Backup and recovery services as Ministry of Finance:

The Ministry of Finance has implemented disaster recovery (DR) capabilities for its critical systems at the Ministry of Innovation Technology's data center. Using built-in Oracle database management system's backup and recovery services feature, data replicate data and transaction logs are configured to remote storage servers. Backup policies and procedures are developed to determine the schedules and frequencies at which the system and data backups will occur.

The key objective of having comprehensive backup and recovery services is to ensure ongoing business continuity for the Ministry of Finance by safeguarding against potential data loss or system downtime. To achieve data protection and rapid restore capabilities, their critical systems and databases are replicated to remote disaster recovery storage located at the Ministry of Innovation Technology's secure data center facilities. By maintaining this remote redundant copy, the Finance Ministry aims to mitigate the risks of any data corruption, infrastructure damage, or errors that could impair systems and data in the primary location. The disaster recovery infrastructure and offsite replicas enable rapid restoration while minimizing disruption in mission-critical finance operations and services.

As researcher's views, in this age of Cyber-attacks, maintaining remote disaster recovery (DR) site for gaining backup and recovery services is mandatory and necessity but not optional for operating mission-critical systems. It is one of security layered preventive mechanism that is defense-in-depth strategy.

Respondent 1 explained that:

> *"We have implemented comprehensive backup and disaster recovery processes for our mission-critical systems. Daily incremental snapshots are replicated into storage servers located at the Ministry of Innovation & Technology. The initial it takes a full back up, then copying changes only since the last replication point. By maintaining this, we guard against localized disruptions either from natural disasters, malicious Cyber-attacks, or other threats that could damage our systems or data integrity."*

As respondent 1 described that, the Ministry of Finance gain benefits and minimized down time of services by implementing reliable backup and recovery services. This ensures the business

continuity by safeguarding against potential data loss in the event of issues with the primary database servers in the main MoF data center.

According to respondent 2 said that:

> *"The implemented a disaster recovery site with the Ministry of Innovation and Technology's data center. The connectivity is connected over dedicated fiber links (dark fiber optics line) to provide high bandwidth and low latency replication. To prevent Cyber-attacks and threats, backups are encrypted both at rest and in transit using strong algorithms. Once up one a time in the past an incident of a denial-of-service (DoS) Cyber-attack was happened on our primary database servers resulting in data loss. So, we were able to completely restore lost data from resilient backups."*

In conclusion, by maintaining reliable and redundant fiber optic connections from different ethio telecom MSG boxes, it can be ensured the reliability and availability of critical backup and recovery services. These provisions serve as the first and last line of defense for safeguarding essential digital assets and building organizational resilience.

4.5.2. Non-Technical Preventive Mechanisms

General concept/idea:

Non-technical preventive mechanisms are critical for building a strong Cybersecurity posture in any organization. Non-technical preventive mechanisms that focus on process, people and best security practices to build a strong security posture. Unlike software and hardware, it is all about educate and ware employees about security threats, risk, compliance to standards, and promote collaboration for knowledge sharing.

Some of non-technical solutions are:

- ✓ **Security Policies & Procedural manuals**: Comprehensive policies and security manuals that provide guidelines on data protection, access controls, email use, endpoint security etc. Ensures consistency in security standards.
- ✓ **Cybersecurity Awareness Training:** Giving awareness training continuously for all employees about general security threats, risks for example how to use strong passwords, identifying phishing attempts etc. and aware about Cybersecurity Unit's security policies and procedures.

- ✓ **Security Audit principles**: Routine comprehensive security procedures to audit and proactively identify gaps, vulnerabilities or non-compliance issues in the security framework.
- ✓ **Security Compliance Frameworks:** Adoption of different industry security standards like ISO 2700 series, NIST, PCI DSS, COBIT, etc that provide guidelines to implement globally accepted security controls.
- ✓ **Knowledge Sharing:** Learning from experiences and best practices around security processes through workshops, seminars from peers and other similar organizations. It helps avoid common pitfalls.
- ✓ And so on.

Non-technical preventive mechanism at Minster of Finance: -Security Policies & Procedure:

In alignment with the national Cybersecurity policy, the Ministry of Finance in collaboration with INSA has developed a suite of security policies (both corporate and issue-specific) as well as standard procedural manuals. Developing these security policies has been a top priority for addressing Cybersecurity issues. This is because comprehensive policies help describe what an organization needs to do to protect its valuable information assets. Well-defined policies put the foundation for securing systems, data, infrastructure and processes that are critical to operations. By outlining clear guidelines around access controls, incident response, employee practices and technical controls, these policies enable organizations to build a robust Cybersecurity framework tailored to its unique risks. As such, formulating strong security policies is a fundamental first step for any entity seeking to enhance its Cyber defense.

According to my assessment as a researcher, the corporate security policy is comprehensive its coverage of both Cybersecurity and physical security domains. The policy shows processes from the main gate to end user desks. Specifically, it describes security protocols related to various stages - hiring new employees (before), during the employee and termination(after) procedures and security clearances when they leave. The goal of this policy is used as framework to secure digital assets, physical infrastructure, and critical systems. I also observed that targeted issue-specific policies and associated procedural manuals have also been developed by the Ministry of Finance for the nine modules under the Integrated Financial Management Information System (IFMIS).

However, I observed some gaps from a policy coverage perspective for certain domain services (that is issue specific policy is not covered or comprehensive all domain services). There is a lack of issue-specific security policies formulated for the remaining departments and services beyond the nine modules under IFMIS that have dedicated issue specific policy and procedural manuals.

According to respondent 1 stated that:

> *"The Ministry has an approved corporate policy along with issue-specific policies that have been formulated for the IFMIS department only so far. These policies were developed in coordination with INSA, based on the Ministry's needs and risk assessment requirements. As per plans, the security policy governance team is expected to carry out risk assessments four times a year. However, due to manpower shortages, these assessments are being done only twice a year at the moment."*

As described by respondent 1, security policies were revised at least once every two years based on the findings from risk assessments. Feedback is also collected from end users to identify any challenges or problems faced in easily implementing these formulated security policies and procedural manuals. And also, the dynamic nature of Cyber security threats, and to alignment with the latest attack mechanisms, updating the security policy is considered mandatory and a necessity. This allows staying on top of emerging risks.

Non-technical PM at Minster of Finance: - Cybersecurity Awareness Training

Although the Ministry of Finance has developed Cybersecurity policies, standard procedures, and implemented the latest technological safeguards, there is a lack of security awareness among employees. Not all employees are yet aware about security issues and existing policies. Even though the Cybersecurity Unit has started conducting awareness training for the top management and senior leadership, as well as domain experts.

In my opinion (searcher), at least, a Cybersecurity awareness training sessions should be conducted to each department and brochures distributed to every employee about aspects like social engineering, email usage, password policies, virus, various form of malware, incident reporting procedures. Building such Cyber hygiene and security-consciousness serves as an effective first-line of defense against numerous Cyber threats and attacks like phishing, social engineering,

malware, data leaks, unauthorized access etc. Awareness at every employee-level will significantly mitigate risks that might bypass technological protections.

Respondent1 described that:

> *"Security awareness training on general Cybersecurity issues and existing security policies and procedures should be conducted for all Ministry of Finance (MoF) employees. The next phase planned is working on more advanced awareness modules focused on human capacity building of the staff. The top management and senior leadership have commitment by supporting such training efforts through allocating required budgets to further strengthen the ministry's Cybersecurity safeguards. For instance, expressed as evidence of such support was, MoF leadership has rented a dedicated training room at the 5killo University Campus. So, we have been giving awareness sessions every week, scheduled in the morning time from 8:30 AM to 9:30 AM for both internal employees as well as external customers who utilize the Ministry's services."*

Continuous Cybersecurity awareness and education for all employees is critical to stay on top of emerging threats. Even with security policies and technical controls in place, there can still be gaps in staff knowledge and skills to properly implement protections. Given induction training at least one month duration for new hire employees as baseline and a general awareness training about security policies and Cyber hygiene. Additionally, regular assessments help identify knowledge gaps that can then be addressed by updating training contents to cover audit and risk assessment findings, while catching up with new threats. A security-conscious organizational culture forms the frontline defense. Without dedicated focus on ongoing and continuous learning about security standards and threats for the entire staff, Ministry's remain vulnerable to zero-day attacks.

Basic idea of from Security Audit principles, Security Compliance Framework & knowledge sharing

The Security Audit team can adopt several principles to ensure a comprehensive approach to auditing and identifying security gaps and weaknesses. Firstly, the audit should take a holistic view of security, encompassing people, processes, and technology. This comprehensive approach allows for a full examination of all aspects of security within the organization. By considering the interaction between these elements, the audit team can identify any vulnerabilities or gaps that may exist.

A risk-based approach is another crucial principle to consider. The audit plans and methodology should prioritize auditing higher-risk areas and assets over others. By focusing efforts on areas that pose the greatest risk, resources can be allocated effectively to address the most critical security concerns. This approach ensures that limited resources are utilized in the most impactful way.

Accountability is also important in the security audit process. When audit findings are identified, it is crucial that those accountable take appropriate corrective actions within reasonable timelines. This accountability ensures that identified weaknesses or gaps are addressed promptly and effectively, reducing the potential for security breaches or incidents.

Continuous learning and improvement are vital components of a robust security audit process. By regularly enhancing the security posture through identified weaknesses, organizations can stay ahead of emerging threats and evolving security challenges. This ongoing improvement process helps to ensure that security measures are continuously updated and adapted to match the changing threat landscape.

Compliance with security policies and industry standards is another key principle for the security audit team. Audits and monitoring should ensure alignment with the Ministry's security policies and relevant industry standards. This compliance ensures that the organization meets the required security standards and minimizes the risk of non-compliance.

Knowledge sharing is an essential aspect of the security audit process. The audit team should actively engage in preparing security awareness training sessions, workshops, and encourage collaboration and open communication regarding security vulnerabilities, issues, and solutions. This knowledge sharing adopts a culture of security awareness and understanding throughout the organization, empowering individuals to contribute to the overall security efforts.

Lastly, developing a formal information security compliance framework based on industry standards and best practices can provide a structured approach to security auditing. Frameworks such as ISO 27000 series, NIST Cybersecurity Framework (CSF), PCI-DSS, and COBIT provide guidelines and benchmarks for organizations to assess their security posture and ensure compliance with established standards.

By adopting these principles, the security audit team can conduct comprehensive audits that identify and address security gaps and weaknesses effectively. This proactive approach to security

auditing helps organizations maintain a robust security posture and minimize the risk of security incidents or breaches.

Non-technical preventive mechanism at Ministry of Finance from Security Audit principles & procedures, enterprise architecture, knowledge sharing culture perspectives are:

MoF has implemented several security practices, for instance, Cybersecurity Unit developed enterprise networking architecture which shows entire business process how to interact each component at high level. They have also strong intensively working on employee's capacity building by preparing training and knowledge sharing. Under Cybersecurity engineering team, there is security audit and evaluation sub-team they formulate security principles and procedures how to they work security auditing job.

The Ministry of Finance (MoF) has implemented various security practices to enhance their cybersecurity measures. For instance, they have developed an enterprise networking architecture that provides a comprehensive overview of how different components interact within the business process. This architecture helps ensure a high level of security throughout the organization.

MoF also prioritizes employee capacity building by offering training and knowledge sharing opportunities. This initiative aims to enhance the skills and knowledge of employees in cybersecurity practices, enabling them to contribute effectively to the organization's security efforts.

Within the Cybersecurity engineering team, there is a dedicated sub-team focused on security audit and evaluation. This sub-team formulates security principles and procedures for conducting security audits. Their role is to ensure that proper auditing practices are followed to identify any vulnerabilities or weaknesses in the system and take appropriate measures to address them.

By implementing these security practices, MoF demonstrates a proactive approach to cybersecurity. Through their enterprise networking architecture, employee capacity building initiatives, and dedicated security audit and evaluation sub-team, they strive to maintain a robust security posture and protect sensitive information and resources.

Respondent 4 stated that:

> *"Before the establishment of the Cybersecurity Unit, there was a lack of centralized management and responsible body for security standards and principles. However, with the*

establishment of the Unit, significant improvements have been made. The security audit and evaluation team within the Cybersecurity Unit have formulated comprehensive security audit principles and procedures. These guidelines provide a structured approach to conducting security audits and evaluations. By implementing these principles and procedures, the organization can ensure that security measures are consistently assessed and improved upon. The establishment of the Cybersecurity Unit has brought about a more systematic and proactive approach to managing security standards and principles within the organization."

In conclusion, besides technical solutions, it is essential to emphasize the importance of non-technical preventive mechanisms to proactively prevent attacks. Building human capacity and development a strong security culture and mindset are particularly crucial in this regard. While technical solutions play a significant role in preventing attacks, non-technical measures are vital for early detection and proactive prevention. Security auditing, on the other hand, is more effective in monitoring and following up after security control systems have been implemented and in response to the emergence of new technologies. By combining technical and non-technical measures, organizations can enhance their overall security posture and mitigate risks effectively.

4.5.3. Physical Control Preventive Mechanisms

4.5.3.1. Security Camera (CCTV) or video surveillance Systems (VSS)

General concept of VSS:

Security cameras, also known as CCTV, are used to capture real-time video footage of premises and record the footage onto storage devices like NVRs and DVRs for monitoring purposes. CCTV systems can utilize digital/IP cameras or analog cameras and come in fixed or PTZ formats that can rotate 360 degrees. Based on shape, CCTV cameras can be bullet cameras or dome cameras.

When any unhealthy activity like theft occurs or when there is unusual activity detected around the compound, floors, data centers, etc. CCTV footage helps easily identify which individuals performed those actions. So, a major functionality of CCTVs that is enabling the identification of objects or people. To make decisions regarding actions taken based on video evidence, the recorded CCTV footage is extremely useful as visual evidence.

Security Camera (CCTV) at Ministry of Finance:

The Ministry of Finance has installed CCTV security cameras to safeguard the entire compound. Dedicated CCTV operators monitor the video feeds from these cameras 24/7. The CCTV coverage includes the data center, corridors on each floor, and the entire compound. The operators keep a watch on every activity and motion captured by the security cameras within these areas. The surveillance provides protection, and the footage can provide evidence if any incidents occur.

On my assessment as researcher, I observed that comprehensive CCTV systems were set up to monitor activities across the entire compound. The CCTV coverage enables easy identification of individuals involved in any illegal actions. The systems also allow 24/7 real-time monitoring of all areas under surveillance.

As respondent 1 said that:

> *"The CCTV security cameras helped us to identify a theft committed by external workers who were working on a project at the office for temporarily. The footage showed this external worker stealing material from a floor. Using the video evidence, the theft who sold the material was recognized."*

CCTV footage serves as evidence whenever any illegal activity takes place. It helps easily identify thefts or unlawful. There is visible warning message displayed walls across all floors stated as **"You are under camera surveillance!"**. This acts as a deterrent to prevent unlawful actions. However, to respect the privacy of employees, CCTVs have not been installed in toilets and within rooms.

4.5.3.2. Access Control Systems (ACS)

Access control systems refer to electronic security systems designed to control and monitor access to entrance into room. The core idea behind access control is to restrict entrance based on established credentials and access rights to ensure that only authorized individuals are able to enter restricted zones.

These systems act as physical security measures that give/deny access right with various combination of PIN plus card reader plus finger print plus eyes iris to detect credentials, electronic locks mounted on doors.

This ACS acts as physical security barriers by leveraging a multilayered approach to verifying credentials before allowing access. These measures include PIN code plus card reader plus fingerprint plus iris scanner, by combinations of these measurements, allow or deny access right to enter into room or restricted area. The defense-in-depth provided by layered access controls provides strengthening protection of sensitive zones, assets and data by restricting entrance only approved personnel.

The data center entrance at the Ministry of Finance has implemented a fingerprint based on access control system. This system allows entry only to authorized personnel who have registered their fingerprints in the system. Without this biometric registration in the access control system, no unauthorized individuals can enter into data center. This access control method has enhanced security measures, replacing the previous method of simple door locks and keys.

4.5.3.3. Fire Alarm System

General concept of Fire alarm system:

A fire alarm system is designed to detect the presence of fire by monitoring environmental changes. Once activated, the system will warm people by alarm soundings of sounders. The system is made up of input devices like smoke, heat detectors that are placed throughout a building. If any of these devices senses a fire, it sends a signal to the system's control panel. The control panel then powers the system's output devices like sounders, bells, warning lights and sends signals to remote monitoring centers.

Fire Alarm System at Ministry of Finance:

The Ministry of Finance has installed a fire alarm system at its data center to protect against fire emergencies or hazards. The system comprises components such as a central control panel, loud alarm sounders, highly sensitive smoke detectors, heat sensors to monitor temperature fluctuations, and gas release actuator connected to cylinder and across each floor’s corridor is put fire extinguishers (it is manual hand-held, it needs human manipulate).

The sensitive detectors have been placed to monitor and transmit warning signals to the central panel at the first sign of smoke or unusual rise in temperature. This automatically activates the loud emergency alarm sounds. At the same time, the release actuators discharge gas from cylinder to contain the fire from spreading. Additionally, multiple hand-held fire extinguishers have also

been kept at easily accessible corridors on each floor. Together, all these enable early detection of fire, timely response to stop fire and prevent major disruptions to operations at the data center due to fire accidents.

In conclusion, the implementation of physical and environmental controlling mechanisms is essential for monitoring activities. The Ministry of Finance (MoF) has installed CCTV security cameras throughout its compound, including the data center and corridor on each floor. As a public service organization, MoF has security personnel at the entrance gate who request identification from customers and guests. CCTV operators continuously monitor all entrances and activities, promptly responding to any suspicious behavior. If any unusual activity is detected, security personnel quickly intervene.

Moreover, when IT personnel enter the data center, they are required to provide their signature, name, and purpose of entry on a prepared form. Similarly, when they exit the data center, they must sign out. Additionally, CCTV cameras within the data center ensure that any unauthorized or inappropriate activity can be easily identified, along with the person responsible. The CCTV footage serves as valuable evidence in the event of an incident or accident.

Therefore, by implementing these measures, MoF ensures a secure environment by actively monitoring and controlling access to its premises, particularly the data center. The combination of CCTV surveillance, strict entry and exit procedures, and the presence of security personnel helps deter potential threats and provides evidence for investigations if necessary.

In conclusion, the preventive mechanisms encompass a various of technical, non-technical, and physical and electronics security control mechanisms which are safeguarding the Ministry of Finance's network infrastructure, systems, data, and physical environments.

Findings, the various preventive mechanisms implemented at MoF are:

- Various **technological enforcement solutions** are employed to enhance security measures. These include using licensed antivirus software to prevent malware attacks, implementing SDN (Software-Defined Networking) technology to improve the data center network infrastructure, and employing AD/DC (Active Directory/Domain Controller) for enforcing centralized policies within the domain users. NAC (Network Access Control) technology is also implemented to mitigate security vulnerabilities and threats associated with Bring Your Own Device (BYOD).

Additionally, firewall security appliances are deployed to filter incoming and outgoing traffic, while WAF (Web Application Firewall) security appliances filter URLs and domains at the application or content level. Load-balancers are utilized to ensure improved availability and performance, and backup and recovery services are employed to guarantee data availability. Data encryption is implemented to prevent data breaches, both when stored (at rest) and during transmission (in motion). Lastly, Identity and Access Control Management (AAA using TACACS or RADIUS protocol server) is implemented for centralized management and configuration of network devices.

- **Non-technical preventive mechanism** measures encompass various strategies. These include establishing security policies, such as corporate policies, issue-specific policies, standard procedures, and guidelines manuals. It is crucial to adhere to security audit principles, rules, and procedures during the auditing process. Compliance with security frameworks and standards is also emphasized. Awareness creation and training programs play a vital role in educating individuals about security threats, vulnerabilities, and preventive measures. Furthermore, promoting knowledge sharing among users through workshops, peer experiences, and collaboration with similar organizations is encouraged.

- Preventive measures related to physical and environmental control encompass several mechanisms. This includes the installation of CCTV security cameras, which enable continuous monitoring to identify individuals engaged in illegal activities like theft. An Access Control System (ACS) is implemented to regulate entry through the data center gate. In addition to ACS, Visitors entering the data center are required to state their purpose of visit, sign in, and sign out upon departure. Fire alarm systems are also installed within the data center to provide protection against potential fires.

4.6. Security Auditing and evaluation

General concept of security auditing and evaluation:

Security auditing is the process of systematically evaluating and testing the effectiveness of security controls and measures in an organization. It involves reviewing the implemented policies, processes, hardware and software (technological solutions) to identify potential weaknesses, risks and areas of improvement.

Security audits on network infrastructure security, endpoint protection, data security, access controls, physical security systems, employee security practices etc and analyzing for vulnerabilities/gaps that could be exploited to compromise systems, steal data or cause other damage. The audits are carried out by specialized security professionals using penetration testing tools, checklists, interviews and inspections.

The findings from security audits shows the gaps that need to be addressed to improve or strengthen security posture over critical systems and sensitive information. The audits help organizations continually assess/evaluate and enhance their information security safeguards, ensuring robust protection mechanisms against Cyber threats.

Security Auditing & evaluation at Ministry of Finance:

A dedicated security audit and evaluation sub-team has been established under Cybersecurity Engineering team of main Cybersecurity Unit to perform security auditing tasks and they formulate auditing principles and procedures aligned to corporate policies. This security audit sub-team conducts periodic assessments of information systems, applications, databases, networks and other technological assets.

The key objectives of security auditing are to findings out any vulnerabilities or gaps in preventive security mechanisms and evaluate it. The audits also evaluate the awareness levels among end-users regarding to general security, Ministry's security policies and procedures. Based on the audit findings, the engineering team provides executable recommendations for remedial actions required to fill the gaps. Over the time, these regular audits help enhance the maturity of the security mechanisms deployed at the Ministry of Finance.

As a researcher, I view security auditing as distinct from IT auditing which deals general over all audit from performance and functionalities of devices rather than security perspective. Security auditing is a technical evaluation focused only on analyzing an Ministry's information systems, security policies, procedural manuals for vulnerabilities from security perspective. Security auditing uses its own security auditing principles, security compliance framework and industry standards such as ISO 27000 series, NIST Cybersecurity Framework, COBIT, PCI DSS etc.

According to respondent 1 said that:

> *"The role of security auditing involves evaluating of the security vulnerabilities and gaps within th*e Ministry's *information systems resources using penetration testing tools. The objective is to identify any weaknesses, such as open ports like telnet (port 21), outdated operating system patches and so on. Once the auditing job is completed, the findings are reported to the Cybersecurity engineering team for remediation and solutions. Additionally, the development directorate is informed of any vulnerabilities found from a software development perspective, enabling them to address and fix the identified issues. This collaborative approach ensures that any security vulnerabilities or gaps discovered during the auditing process are promptly addressed and resolved."*

To sum up, security audit jobs primarily are focused on assessing/evaluating the vulnerabilities or gaps in information systems and security policies; it is from security aspects. Security auditing is a specialized area within IT auditing jobs that addresses both security and performance issues related to information systems.

The Security audit and evaluation at MoF also conducts regular security assessments, vulnerability scanning, and penetration testing to proactively identify and address any security weaknesses or vulnerabilities. It collaborates with other departments, such as the Cybersecurity engineering team and the development directorate, to ensure that security measures are implemented and vulnerabilities are remediated effectively.

Findings, at the Ministry of Finance (MoF), the Cybersecurity unit includes a Security Auditing and Evaluation team that conducts security audits and evaluations. These audits are based on risk assessments and aim to identify any gaps or vulnerabilities in systems and technology after their implementation. The team utilizes cybersecurity penetration tests, also known as ethical hacking, to assess the vulnerabilities of the systems. In the event that gaps are identified, the team takes immediate action by initiating incident response or remediation measures, commonly known as "hardening," to address and resolve the vulnerabilities. Therefore, establishing a security auditing and evaluation process brings positive factors that enhance and ensure the overall security posture.

4.7. Security Operation Center (SOC)

General concept of SOC:

A Security Operation Center (SOC) is a centralized unit within an organization that is responsible for monitoring, detecting, and responding to security incidents and threats. It serves as a command center where security analysts and experts use various tools and technologies to continuously monitor the organization's networks, systems, and applications for any signs of unauthorized access, malicious activities, or anomalies. The SOC plays a critical role in maintaining the organization's security posture by quickly identifying and responding to security incidents, minimizing the impact of potential breaches, and ensuring the overall protection of sensitive information and assets.

SOC at Ministry of Finance:

The Ministry of Finance (MoF) has implemented dedicated Security Operation Center (SOC), which is a centralized unit responsible for monitoring, detecting, and responding to security incidents and threats within the organization. The SOC utilizes commercial licensed technologies, tools, and to continuously monitor the MoF's networks, systems, and applications for any signs of unauthorized access or malicious activities.

The SOC at MoF plays a crucial role in maintaining the security posture of the organization. It actively monitors and analyzes network traffic, logs, and security alerts to identify potential security incidents. Once an incident is detected, the SOC initiates an incident response process, working closely with the relevant teams to investigate, contain, and mitigate the impact of the incident.

Overall, the SOC at MoF plays a critical role in safeguarding the organization's sensitive information, assets, and infrastructure from potential cyber threats and attacks.

According to respondent 5 said that:

> *"They have implemented a 24/7 monitoring system that continuously monitors and analyzes inbound and outbound traffic in real-time. If any unusual traffic patterns are detected, it is reported to the incident response team."*

However, the respondent 5 also mentioned that there is a lack of skilled security analysts at the moment. This is primarily due to the department being new and lacking experience. To compensate for this, they have been working in collaboration with the ISNA Ethio-cert team to ensure effective monitoring and incident response.

According to the respondent 4 said:

> *"Information asset classification has been conducted to facilitate the monitoring of inbound and outbound traffic. The classification is primarily based on the critical systems of the MoF, such as IFMIS and EGP systems. However, the focus on monitoring regular Internet users' traffic is not as significant at the moment."*

According to the description provided by respondent 4, the monitoring of traffic is carried out based on a predefined information classification. The main focus is on monitoring the inbound traffic of critical systems, as most of the MoF's customers access these systems via the Internet.

Findings, the Ministry of Finance (MoF) has established an independent Security Operation Center (SOC) team dedicated to monitoring real-time inbound and outbound traffic for selected sensitive systems. Within MoF, information assets have been categorized, with critical digital finance systems such as E-GP and IFMIS assigned high-risk levels. This categorization for ordinary Internet users within MoF is low risk they put. The SOC team conducts log analysis to identify any suspicious or unusual patterns within the results. Once detected, these patterns are promptly reported to the Detection Response Team (CER^2T), which operates under the Cybersecurity Engineering team. This setup ensures that the MoF can effectively monitor and respond to potential security incidents, safeguarding their critical information assets.

Hence, establishing a dedicated Security Operation Center (SOC) team at the Ministry of Finance (MoF) brings several positive factors that contribute to enhancing the overall security posture.

4.8. Proposed Information System Security Framework

The purpose of this study was to investigate the information system security practices in the Ministry of Finance (MoF). With increasing digital connectivity, information has become the main critical resource of the organization. This resource has to be protected from all sorts of cyber security threats. The framework has six components as shown in the following.

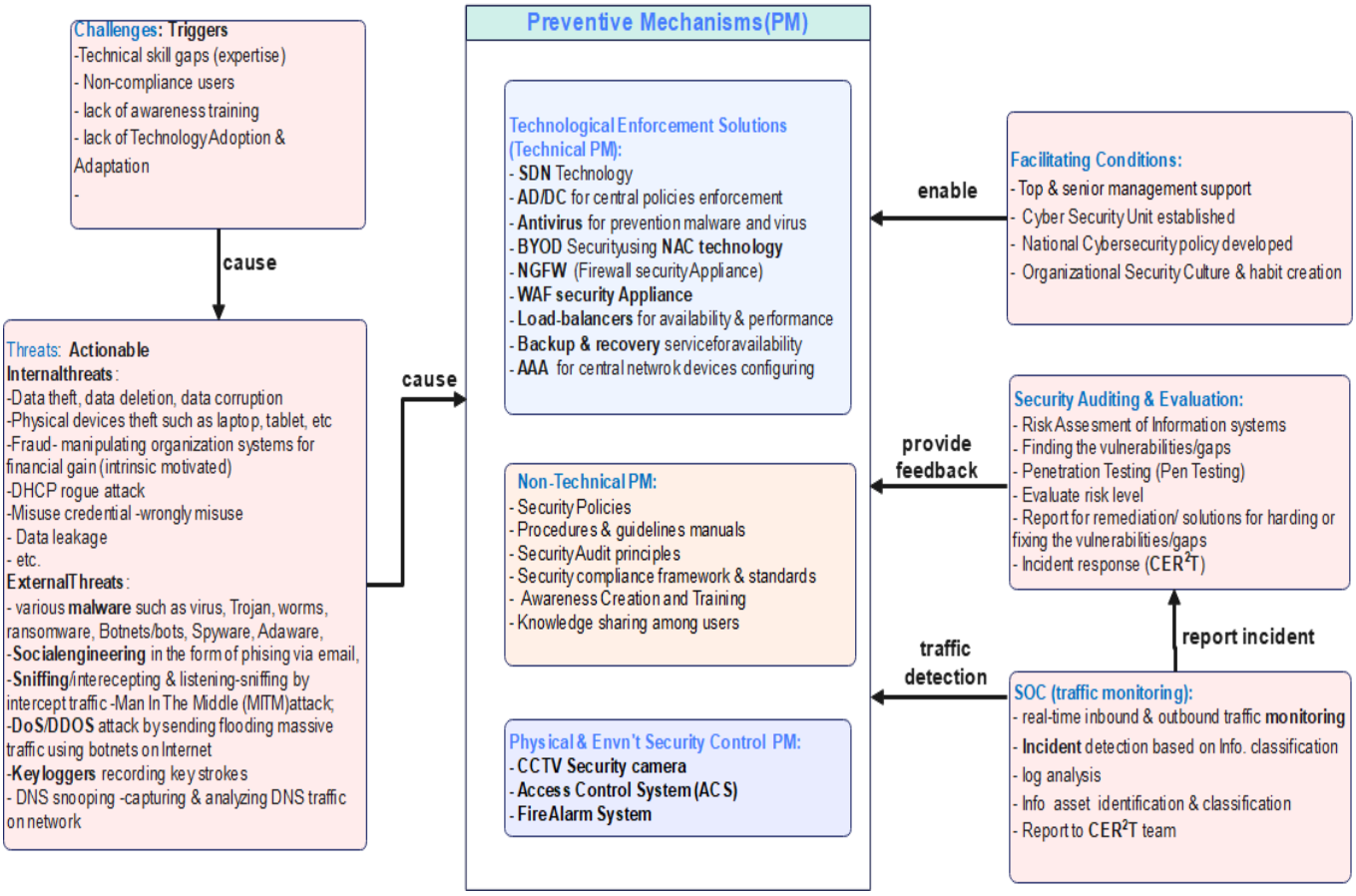


***Figure 4-1**: Proposed Information System Security Framework*

Information security challenges:

Challenges refer to the problems, issues, obstacles, barriers or difficulties that an organization faces during implementing, operating, governing, and securing security policies, standard procedures, and a new technological solution. Because implementing and practices of information security is always ongoing process with challenges. In the case of Ministry of Finance, MoF handles a vast amount of sensitive digital financial data, making it an attractive target for cybercriminals.

Some common potential difficulties an organization has faced or encountered during security practices include Legacy systems that can be challenging to be update, upgrade and secure. For example, older network devices like Cisco 2960 switches) that are passed the end-of-life that is end-of-product, end-of-support which means dead device with no more new patches released, old computers and laptops may be difficulties to upgrade from Windows 7 to newer Windows 10 and

11. Lack of Cybersecurity professionals and personnel skilled, experienced for newer technologies like SDN technology that has been adopted. Another issue is an insufficient user's awareness training on security policies and lack of general security and inadequate budget and management support for buying network devices and training, and more.

Therefore, the interaction and relationship between information security challenges and threats can be seen as **cause-and-effect**. Information security challenges act as pre-conditions or triggers that can lead to the occurrence of threats. Challenges create the circumstances or vulnerabilities/gaps that make it possible for threats to be happened. In other words, the challenges faced by an organization in maintaining information security can create the conditions that allow threats to be potentially exploit weaknesses in the security measures. Therefore, addressing and mitigating the information security challenges is crucial to prevent or minimize the occurrence and impact of threats.

Information system security threats:

Some of the challenges associated with legacy systems, which are challenging to update, upgrade, secure. This leads to security threats and attacks. The lack of cybersecurity professionals skilled in newer technologies like software defined networking (SDN) and inadequate awareness training on general security policies. This has resulted to employee's failure to adhere to security policies and procedures. So, several employees prioritize completing tasks without integrating a security mindset into their regular work. The existing security policies does not cover all MoF's domain services is another bottleneck.

The findings of the study revealed different information security threats. These are lack of comprehensive awareness training on security policies and procedures, lack of skilled Cybersecurity professionals, lack of commitment and dedication from employees to adhere to organizational security policies and procedures. There is also an unwillingness to adapt and adopt new technologically solutions.

The findings that have gotten from the data analysis on threats are: in terms of digital threats, the analysis report identifies common cyber threat categories such as malware, virus, Trojan, social engineering, phishing, denial-of-service attacks, data breaches, brute force attacks, zero-day threats, insider threats, as well as use computer and network device weak passwords. These threats can lead to the compromise of computing systems, networks, and devices to disrupt operations and

unauthorized access, data theft, and financial fraud. The analysis report suggests implementing measures like multi-factor authentication, strong password policies, firewalls, intrusion prevention systems, software updates, Active director/domain controller, antivirus software, network access device for endpoint devices security protection, backup and recovery services, user education, and overall robust security countermeasures to mitigate these threats. The physical threats that the MoF has faced that compromise physical assets and infrastructure, such as theft, fires, and equipment failure, including unlocking of each floor wall rack.

The relationship and interaction between information security threats and preventive mechanisms can be seen as cause-and-effect. The existence of threats necessitates the implementation of security control mechanisms, whether they are technical or non-technical solutions. Threats act as the driving force behind the creation and implementation of preventive measures. In other words, the identification of potential threats prompts organizations to develop and deploy preventive mechanisms to mitigate the risks associated with those threats. Therefore, threats are the catalyst for the establishment of preventive measures in information security.

Information security prevention mechanisms:

As data analysis reveals various threats faced by the Ministry of Finance (MoF), both in physical and digital forms. The report emphasizes the importance of implementing multiple layered technical and non-technical controls to protect the confidentiality, integrity, and availability of critical infrastructure and sensitive information. The respondents emphasized the importance of continuous training, verifying the security posture of devices, and implementing preventive controls like antivirus software and use multi-factor authentication.

Prevention mechanisms are proactive measures implemented to prevent threats from compromising the security of information assets, providing organizations with a strong defense against potential security incidents. The relationship between prevention mechanisms and threats is crucial in robust solutions to mitigate potential threats and risks. By identifying and understanding the nature of threats, organizations can implement appropriate prevention mechanisms to address specific risks effectively.

Facilitating conditions for enabling of InfoSec preventive mechanisms:

The focus of the data analysis report was on the factors that support the implementation of effective information security preventive mechanisms. The Ministry of Finance demonstrates strong leadership and top management support by allocating an adequate budget for a dedicated Cybersecurity unit and ensuring compliance with national policies. The commitment of top management is evident through their support for upgrading the network infrastructure using SDN technology, implementing advanced security measures like NAC and WAF, and providing awareness training.

These facilitating conditions empower the Cybersecurity unit to effectively carry out its mission. It is important to allocate sufficient budget and resources for modern security technologies and to enforce accountability for non-compliant users. User awareness programs and training, along with a dedicated Cybersecurity unit responsible for auditing and monitoring the security posture, also contribute to creating facilitating conditions. Additionally, it is crucial for corporate security policies to align with national Cybersecurity policies.

The overall, facilitating conditions play a key role in fostering a shared cybersecurity culture among employees, conducting continuous security awareness training, and implementing robust technical controls. These conditions also involve non-technical solutions to proactively prevent attacks.

Therefore, facilitating conditions refer to factors or conditions that enable or contribute to the security preventive mechanisms.

The relationship between facilitating conditions and preventive mechanisms is enabling because identifying and addressing facilitating conditions is crucial for the effectiveness of preventive measures. By leadership and top management supportive, commitment and dedication organizations can strengthen their security posture and empower their preventive mechanisms to effectively counter potential threats as well as successful implementation and operation of preventive mechanisms.

Information security non-technical preventive mechanisms:

The discussion focused on non-technical preventive mechanisms for effective enhancement of information security practices. These mechanisms include security policies and procedural manuals, cybersecurity awareness training, security audit principles, security compliance

frameworks, and knowledge sharing among employees. Security policies and procedural manuals provide guidelines on data protection, access controls, email use, and endpoint security. They ensure consistency in security standards and form the foundation for securing systems, data, infrastructure, and critical processes. Cybersecurity awareness training is essential for educating employees about general security threats, such as phishing attempts, and promoting adherence to security policies and procedures. It helps build a security-conscious organizational culture and serves as a first-line defense against various cyber threats. Security audit principles involve routine comprehensive procedures to identify gaps, vulnerabilities, or non-compliance issues in the security framework. By taking a holistic view of security across people, processes, and technology, audits help enhance the security posture and ensure accountability for corrective actions.

Adopting security compliance frameworks, such as ISO 27000 series, NIST, PCI-DSS, and COBIT, provides guidelines to implement globally accepted security controls. These frameworks help organizations align with industry standards and best practices. Knowledge sharing through workshops, seminars, and collaboration with peers and other organizations allows for learning from experiences and best practices. It helps avoid common pitfalls and enhances the effectiveness of security processes.

Hence, although non-technical preventive mechanisms in information security are a sub-component that supports technical preventive solutions, their importance and necessity cannot be overstated.

Physical and Electronics Security Preventive Mechanisms:

The data analysis report focused on the main theme of Physical and electronics security control Preventive Mechanisms, which are security cameras (CCTV), access control systems, fire alarm systems. These measures helped deter unlawful actions, identify and capture criminals, control access to sensitive areas, detect and respond to fire emergencies, and continuously improve the security mechanisms in place.

Since security cameras provided 24/7 real-time monitoring and allowed for easy identification of individuals involved in illegal activities. The footage from the CCTV cameras also served as valuable evidence in identifying and capturing a thief who had stolen materials from the office.

The access control systems (ACS), the data center entrance gate at the Ministry of Finance implemented a fingerprint-based access control system. This system only allowed entry to

authorized personnel who had registered their fingerprints. This biometric registration enhanced security measures compared to traditional door locks and keys, ensuring that only authorized individuals could access the data center.

As a core element of preventive mechanisms within the broader information security framework, both physical and electronic security control mechanisms hold significant importance. They are integral components that contribute to the overall security of an organization's information assets.

Information security preventive mechanism: - Security Auditing and evaluation:

According to the data analysis report, security auditing and evaluation are conducted in the Ministry of Finance (MoF) to systematically assess and test the effectiveness of security controls and measures. These audits aim to identify potential weaknesses, risks, and areas for improvement in policies, processes, hardware, software, and employee practices.

As part of the auditing process, log analysis is performed to monitor and analyze system activity. If any unusual traffic is detected, it is reported to the cyber engineering response team for remediation and solutions. Additionally, the system development directorate is involved in fixing or strengthening vulnerabilities from a software development and implementation perspective. This collaborative effort ensures that both teams work synergistically to address security issues and enhance the overall security posture of the MoF.

The relationship and interaction between the Security Auditing and Evaluation component and preventive mechanisms involve providing feedback for further security preventive enhancements. The key theme of Security Auditing and Evaluation is to assess the effectiveness of preventive control mechanisms through audits and evaluations. The audit results serve as feedback to identify areas for improvement in the preventive measures, allowing organizations to enhance their security controls and strengthen their overall security posture.

Information security preventive mechanism: - Security Operation Center (SOC):

Security Operations Center (SOC) at the Ministry of Finance (MoF) from an information security practices perspective would involve examining the role and functions of the SOC in ensuring the security of MoF's information assets.

The SOC at MoF plays a critical role in monitoring, detecting, and responding to security incidents and threats. It operates 24/7 and utilizes commercial licensed technologies and continuously

monitor the MoF's networks, systems, and applications. The SOC analyzes real-time inbound and outbound traffic, identifies any unusual or suspicious activities, and promptly reports them to the incident response team for further investigation and mitigation.

From an information security practices perspective, the SOC at MoF should have well-defined processes and procedures in place. This includes incident response plans, communication and reporting protocols to ensure effective coordination and response to security incidents. Regular training and skill development programs should be provided to SOC analysts to keep them updated with the latest security trends and techniques.

The SOC should also collaborate closely with other departments within the MoF, such as the IT support department and the development directorate to ensure that security measures are implemented throughout the organization's infrastructure and applications. This includes conducting regular security assessments, vulnerability scanning, and penetration testing to identify and address any weaknesses or vulnerabilities.

So, the SOC team proactively detect and respond to emerging threats and ensure the MoF's information assets are adequately protected.

Overall, the discussion around the SOC at MoF from an information security practices perspective should focus on its role, processes, collaboration with other departments, and continuous improvement to enhance the overall security posture of the organization.

Hence, the relationship and interaction between the Security Operations Center (SOC) component and the preventive mechanism component involve log analysis and traffic detection. The SOC monitors incoming and outgoing traffic by analyzing logs and, if any unusual traffic or incidents are detected, it promptly reports them to the Computer Emergency Response Team (CERT) for further investigation and response.

In conclusion, the presented research aimed to develop comprehensive ISS framework that combines organizational, technological, and individual aspects rather than isolation by identifying these critical factors from empirical data on existing information system security prevention practices at the Ministry of Finance (MoF). However, there are a lot of other established InfoSec frameworks, such as ISO 27001, this study was focused on the organizational context at the Ministry of Finance.

The international one is more complex and cannot be implemented in an Ethiopian context. The proposed framework emerges from the empirical data so that it has better explanatory power for the organization's security systems. This proposed framework is also a lightweight framework that can be easily implemented by cybersecurity practitioners, cyber security experts, policymakers, etc.

4.9. Evaluation of proposed information System security framework (Report)

To evaluate the proposed information system security framework at the Ministry of Finance (MoF), an evaluation checklist was prepared as shown in the appendix IV section. This checklist was served as a tool to assess the effectiveness and completeness of the framework. By systematically reviewing each component and requirement of the framework against the checklist, it was possible to identify any gaps or areas that require improvement. This evaluation process was provided the valuable insights into the strengths and weaknesses of the proposed framework, enabling necessary adjustments and enhancements to ensure its efficacy in safeguarding the MoF's information assets.

Respondent 1 said that:

> *"Since the organization did not have an existing security framework, the proposed framework is comprehensive and serves as a suitable starting point. This is because the framework incorporates the organization's current security practices as its components."*

Overall, Respondent 1 viewed that the proposed framework helps MoF to systematically identify and categorize various elements, such as threat triggers under the threat component, challenges under the challenge component and so on.

According to respondent 2 said that:

> *"Additionally, he has identified and suggested the need for dedicated a Security Operations Center (SOC) component, which was previously combined with security auditing and monitoring functions."*.

By taking the respondent 2's recommendation and suggestion into the account, then the researcher added the SOC component on proposed framework since it has been acceptable by the MoF's cybersecurity experts and professionals for implementation in their information system security practices.

Respondent 3 said that:

> *"The proposed framework clearly showcases the organization's current security practices, including the responsibilities and accountabilities of different bodies within the organization. This helps to empower the organization's duty segregation, which is a crucial aspect of effective information security management."*

By clearly mapping the existing security practices and the associated roles and responsibilities, the framework provides a structured and transparent view of the organization's security landscape. This clarity can help to strengthen the organization's security governance, ensuring that there is a clear delineation of duties and accountability for various security-related tasks and decisions.

In conclusion, after evaluation of the several more than three Cybersecurity experts and professionals at the Ministry of Finance (MoF), the proposed framework has received positive feedback as being good and workable for their Information System Security practices.

As researcher, for further confirmation of framework's usability, effectiveness, and practicality, I have shown them different use cases that derived from this proposed framework.

CHAPTER FIVE

CONCLUSION and FUTURE RECOMMENDATIONS

5.1. Introduction

This study focused on the problems and objectives related to developing information system security framework specifically for Ministry of Finance (MoF). In chapter two, conducted the literature review to explore and examine the current or existing state of Information System Security and cybersecurity within financial institutions, with emphasizing the significance of trust and credibility in this sector. Then chapter three and four, research methodology and data analysis were discussed.

Financial institutions face unique challenges in cybersecurity due to their public-facing products and services, as well as the volume of sensitive customer information they handle. Common cyber threats include data breaches, identity theft, fraudulent transactions, and system downtime. In this research, an information system security framework was developed specifically for the Ministry of Finance (MoF). The framework's effectiveness was evaluated, and it was found to be highly relevant for implementation.

This chapter also includes a summary of the research findings and contributions. It acknowledges the limitations of the study and provides recommendations for future research. Finally, this chapter concludes the study by discuss in the importance of implementing the developed information system security framework to enhance the security and protection of information system security in MoF.

5.2. Research Conclusion

The primary objective of this study was to develop an Information System Security framework specifically designed for the Ministry of Finance (MoF) in Ethiopia. The proposed framework was evaluated by MoF's domain experts from their institution perspective. As the analysis revealed that, Cyber-risk is an emerging threat that affects all financial institutions. By providing a roadmap of framework for addressing Information System Security issues, this study contributes to the body

of knowledge on Information System Security for financial institutions, particularly in the Ethiopian.

The study identified key influential factors necessary for enhanced Information System Security practices to safeguard the MoF's information systems, and the developed Information System Security Framework plays a crucial role in building cyber resilience. This study explored and analyzed Information System Security practices, international industry standards and frameworks, finally developed a framework tailored to the specific financial institution of MoF. The proposed information system security framework consisted of six major components and its respective sub-components. These six components and its sub-components were identified from the empirical data collected through interview and document review.

The first finding was challenges, which include the absence of comprehensive awareness training on general security practices, security policies (both corporate and issue-specific), and procedures. Another challenge identified is the lack of technical skills, particularly the shortage of certified cybersecurity professionals capable of addressing the rapidly evolving landscape of emerging cybersecurity threats, such as zero-day attacks, and implementing various prevention mechanisms.

The second finding was the common threats that found in MoF. These threats are included the various form of malware such as viruses, worms, Trojan, ransomware, spyware and adware. Additionally, the identified threats include fraud, denial-of-service (DoS) attacks, and social engineering attacks, specifically phishing attacks through email and impersonation of legitimate individuals or trusted friends during social interactions.

The third finding was the importance of top management support, dedication, and commitment. This support is verified through the allocation of budgets for purchasing necessary devices, licensed software (such as operating systems, antivirus programs, and SSL certificates for securing web browsers), allowed to upgrading network infrastructure projects, developing security policies and procedures, and conducting capacity-building employee awareness training. Furthermore, the establishment of a dedicated Cybersecurity unit was found to be facilitated by the crucial roles played by top management. This component, categorized as "facilitating conditions," represented in the proposed information system security framework.

The fourth finding that emerged was the implementation of various technical and non-technical preventive measures within the Ministry of Finance (MoF) as a financial institution. In terms of

technological enforcement solutions, the MoF has implemented next-generation firewalls for internal and external protection, web application firewalls (WAF), active directory/domain controller (AD/DC), licensed commercial server-based antivirus software, Software Defined Networking (SDN) technology for optimizing data center network infrastructure, network access control (NAC) technology for securing bring your own device (BYOD) vulnerabilities, centralized network device configuration and management using authentication authorization auditing (AAA), backup and recovery services (including a Disaster Recovery (DR) site), load-balancers for availability and performance and more.

In addition to the technical measures, non-technical prevention techniques have been used. These include the establishment of security policies and standard procedures, the development of comprehensive awareness training on general security practices and security policies, the development of enterprise network architecture that shown entire business process, adherence to international and industry Information System Security frameworks and standards, security auditing and principles, compliance with Information System Security standards, fostering knowledge and experience sharing among employees and similar organizations, and the cultivation of organizational security practices and habits. Furthermore, physical and environmental security controls such as video surveillance systems, access control systems, and fire alarm systems have been implemented.

The fifth finding identified in the study was related to security auditing and evaluation. This involves conducting risk assessments to identify gaps and vulnerabilities in the network infrastructure and information systems. These gaps are then categorized based on their risk level, whether it is medium, high, or low. Feedback is provided for remediation and solutions to address the identified risks.

The sixth finding was the establishment of a Security Operations Center (SOC). A dedicated SOC team is 24/7 hours continuously monitoring the real-time inbound and outbound traffic. If any unusual traffic patterns are detected, it is reported to the relevant detection response team for further action.

In conclusion, this study findings may help Ministry of Finance to improve and enhance their information system security practices and compliance for protecting and safeguarding of critical

network infrastructure, information systems, sensitive information asset and its customers data by ensuring the continuity of vital financial services.

5.3. Research Contributions

This research theoretical contribution is the proposed information system security framework. This framework was used as lens by other researchers when they study Information System Security practices outside the financial institution sectors.

The framework has also relevance for managers and security workers to improve their security practices and protect their system from different security attacks, etc. It helps them to save millions of dollars from being wasted due to security breaches, etc. And also, this developed information system security framework serves as a valuable resource for MoF's Cybersecurity teams to formulate different several use case scenarios for security practices.

5.4. Research Limitations

The primary constraint of this study was the time limitation, which is not carried out all financial institutions in Ethiopia. To address this limitation, a case study design focusing on a single organization, MoF, was chosen. However, this narrowed the scope of the study to only one institution. Additionally, the study faced constraints in terms of budget and resources, which were not easily available. As a result, it was not feasible to conduct a comprehensive evaluation of the framework's effectiveness in other financial organizations.

5.5. Future Recommendations

The recommendations for further study include similar research in other business sectors of Ethiopia using the proposed information system security framework as a reference. Other researchers can also validate the framework with quantitative research methodology for its generalizability.

The researcher also recommends the following areas for future research:

- Investigate Bring Your Own Device (**BYOD**) security protection from a cyber-threat and attack perspective. This approach can provide insights into important factors such as the intentions and motivations of attackers, target selection and exploitation choices, as well as perceptions related to cyber defense within an organization's infrastructure.

- Conduct a study on Data Loss Prevention (**DLP**) techniques that aim to prevent data breaches and leakages. This research can explore into the effectiveness of different DLP measures, such as encryption, access controls, and monitoring systems, to safeguard sensitive information leakages and stealing.
- Evaluate the effectiveness of the implemented information system security frameworks, standards and security awareness training for employees and users: Conduct a comprehensive assessment of the framework's impact on improving information system security practices within the organization.

These areas of research can contribute to a better understanding of BYOD devices vulnerabilities, zero-day attacks, enhance and improve data protection measures, information/cyber security practices, security culture and habit.

Bibliography

Acocella, I. (2012). The focus groups in social research: advantages and disadvantages. Quality & Quantity, 46(4), 1125–1136.

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Akamai Technologies, Inc (2018). Akamai State of the Internet: Web Attack Report Shows Hospitality Industry Under Siege from Botnets.

Alotaibi, T., Furnell, S. (2016). Assessing Staff Acceptance and Compliance with Information System Security. International Journal of Computing Academic Research (IJCAR), 5(4), 195-201.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security Compliance in Organizations: An Institutional Perspective. Data and Information Management, 1(2), 104-114. Received on January 08, 2024 from https://doi.org/10.1515/dim-2017-0006

AlKalbani, A., Deng, H., and Kam, B. (2015). Organizational security culture and information security compliance for e-government development: the moderating effect of social pressure. Association for Information Systems (AIS), 1-11.

Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. English Linguistics Research, 3(1), 39–45.

Antoniou, G. (2015). Designing an effective information security policy for exceptional situations in an organization: An experimental study.

Andrade, A. D. (2009). Interpretive research aiming at theory building: Adopting and adapting the case study design. The Qualitative Report, 14(1), 42-60.

Bhagat, S., Kim, K., and Guerra, K. (2020). BYOD Security Policy Compliance: Role of Policy Awareness, Organizational Culture and Social Controls. *AMCIS Proceedings* 15. Received on January08,2024fromhttps://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/15

Bhasin, M. L. (2015). Menace of frauds in the Indian banking industry: An empirical study. Australian Journal of Business and Management Research, 4(12), 1-13.

Borrion, H., & Yuryna Connolly, L. (2020). Your money or your business: Decision-making

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Bulgurcu , B., Cavusoglu, H., Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

Carmi, G., Bouhnik, D. (2021). Behavioral Factors That Influence Employees to Comply with Information Security Policies. Journal of Internet Technology and Secured Transactions (JITST), Volume 9, Issue 1, pp. 722-724.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. Oncology Nursing Forum, 41(5), 545-547.

Center for Internet Security (CIS). (2018). CIS controls. Retrieved on January 08, 2024 frohttps://www.cisecurity.org/

Chochliouros, I. P., Spiliopoulou, A. S., Stephanakis, I. M., Arvanitozisis, D. N., Sfakianakis, E., Belesioti, M., … Mitsopoulou, N. (2015). Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also focusing upon the Cloud Perspective. In Proceedings of the 16th International Conference on Engineering Applications of Neural Networks (INNS) (p. 28).

Collis, J., & Hussey, R. (2013). Business research: A practical guide for undergraduate and postgraduate students. Macmillan International Higher Education.

Committee on Payments and Market Infrastructure (CPMI). (2016). Board of the International Organization of Securities Commissions (IOSCO): Guidance on cyber resilience for financial market infrastructures. Bank for International settlements. CPMI-IOSCO.

Committee on Payments and Market Infrastructures (CPMI**).** (2016). Guidance on cyber resilience for financial market infrastructures.

Cram, W.A., D'Arcy, J., & Proudfoot, J.G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525-554.

Creswell, J. (2014). Research design: Qualitative, quantitative, and mixed methods approach (4th ed.). Sage.

Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing among five approaches. Sage publications.

Crisanto, J.C., & Prenio, J. (2017). Regulatory approaches to enhance bank's cyber-security frameworks. Financial Stability Institute insights on policy implementation No 2: Bank for international settlements.

De Hoyos, M., & Barnes, S. (2014). Analyzing interview data. Warwick Institute for Employment Research.

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. Nurse researcher, 20(5), 28-32. doi: 10.7748/nr2013.05.20.5.28.e327

Eloff, M.M and von Solms, S.H. (2000). Information Security Management: A Hierarchical Framework for Various Approaches. Computers & Security, 19(3), 243-256.

Erastus, L., Jere, N., & Shava, F. B. (2017). A security model for Namibian Government Services. In IST-Africa Week Conference (IST-Africa), 1–11.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1–4.

Executive Order. (2013). Executive Order 13636: Improving Critical InfrastructureCybersecurity.

White house Presidential Documents, 78(33).

Girma, A. (2020). A Framework for Human Factors Influence on Information Systems Security at Commercial Banks in Ethiopia. Addis Ababa University.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. European Journal of Information Systems, 21(2), 135–146.

Gray, D. E. (2014). Doing research in the real world. 3rd ed, Sage.

Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106- 125.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Information and Management, 51(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

Information Network Security Agency (INSA). (2016). Computer Crime Proclamation No. 958/2016. FEDERAL NEGARIT GAZETTE OF THE FEDERAL DEMOCRATIC REPUBLIC OFETHIOPIA.https://www.insa.gov.et/web/guest/%E1%88%B0%E1%8A%90%E1%8B%B6%E1%89%BD

Information Network Security Agency (INSA). (2011). National Information Security Policy.

Information Network Security Agency (INSA). (2022). National Cybersecurity Policy & Strategy.

Information Systems Audit and Control Association (ISACA). (2019). COBIT 2019 Framework: Introduction and Methodology.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.

International Organization for Standardization (ISO). (2022). ISO/IEC 27002:2022 - Information technology - Security techniques - Code of practice for information security controls. International Organization for Standardization.

International Telecommunication Union (ITU). (2016). ICT Facts and Figures 2016.

Kaspersky Lab. (2019). Kaspersky Lab financial cyber threats report. Received on January 08, 2024fromhttps://usa.kaspersky.com/about/press-releases/2019_kaspersky-lab-financial-cyberthreats-report

Khan, S. R. (2018). Implication of cyber warfare on the financial sector. An exploratory study. International Journal of Cyber-Security and Digital Forensics, 7(1), 31–38.

Kizza, J. M. (2019). Guide to Computer Network Security (4th ed.). Springer.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. Computers & Security, 33, 3-11.

Kothari, C. R., & Garg, G. (2014). Research methodology and techniques. New Age Internationals Publications.

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. Journal of Information Assurance & Cybersecurity, 1.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. Health Promotion Practice, 16(4), 473–475.

Li, J. X. (2017). Cybercrime and legal countermeasures: A historical analysis. International Journal of Criminal Justice Sciences, 12(2), 196–207.

McIlwraith, A. (2006). Information security and employee behavior: how to reduce risk through employee education, training and awareness. Gower Publishing, Ltd.

Merriam, S. B., & Tisdell, E. J. (2016). Qualitative research: A guide to design and implementation. John Wiley & Sons.

MOHAMMED, D. (2018). Cybersecurity compliance in the financial sector. The Journal of Internet Banking and Commerce, 20(1), 1–11.

Moody, G.D., Siponen, M., and Pahnila, S. (2018). Toward a unified model of information security policy compliance. Mis Quarterly, 42(1), 285-311.

Moynihan, D. P. (2004). Building Secure Elections: E-Voting, Security, and Systems Theory. Public administration review, 64(5), 515-528.

Muganda, N. (2010). Applied business and management research: Exploring the principles and practices of research within the context of Africa.http://repository.tukenya.ac.ke/handle/123456789/1185

Myers, M. D. (1997). Qualitative Research in Information Systems. MIS Quarterly, 21, 241-242.

National Institute of Standards and Technology (NIST). (1996). Generally Accepted Principles and Practices for Securing Information Technology Systems; SP 800-14; NIST: Gaithersburg, MD, USA.

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical Infrastructure Cybersecurity.https://csrc.nist.gov/pubs/cswp/6/cybersecurity-framework-v11/final

Nieles, M., Dempsey, K., Pillitteri, V. (2017). An Introduction to Information Security. NIST Special Publication 800-12 Revision 1. https://doi.org/10.6028/NIST.SP.800-12r1

Nord, J., H., Koohang, A., Floyd, K., Paliszkiewicz, J. (2020). IMPACT OF HABITS ON INFORMATION SECURITY POLICY COMPLIANCE. 21(3), 217-226.

Payment Card Industry Security Standards Council PCI-DSS, (2019). Payment Card Industry Data Security Standard (PCI DSS) Version 3.2.1.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. MIS quarterly, 757-778.

Qatar Ministry of Transport and Communications (MOTC) Cyber Security Policy and Standards. (2018). Bring Your Own Device (BYOD) Security Policy, version 1.1.

Rahman, A., & Abedin, M. J. (2021). The Fourth Industrial Revolution and private commercial banks: The good, bad and ugly. International Journal of Organizational Analysis, 29 (5), 1287-1301. https://doi.org/10.1108/IJOA-05-2020-2218

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and INFORMATION SECURITY IMPLEMENTATION 210 operationalization. Quality & Quantity, 52(4), 1893–1907.https://doi.org/10.1007/s11135-017-0574-8

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, (6th ed.) London: Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for business students (7th ed.). Edinburgh Gate: Pearson Education Limited.

Security Intelligence (2016). Security Intelligence. Retrieved on January 08,2024 from https://securityintelligence.com/five-cybersecurity-challenges-facing-financial-services-organizations-today/

Semlambo, A., A., Lubua, E., W., Mkude, C., G. (2022). Factors Affecting the Security of Information Systems in Africa: A Literature Review. University of Dar es Salaam Library Journal, 17(I2), 94-114.

Temtim, A., Alpha, T. (2021). Factors influencing information security compliance: an institutional perspective. SINET: Ethiop. J. Sci., 44, 108–118.

Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2017). Is NIST CSF applicable for developing nations? A case study on Government Sector in Malaysia. PACIS Proceedings. 101.http://aisel.aisnet.org/pacis2017/101/

Thanh, N. C., & Thanh, T. T. (2015). The interconnection between interpretivist paradigm and qualitative methods in education. American Journal of Educational Science, 1(2), 24–27.

Tornatzky, L. G., Fleischer, M., and Chakrabarti, A. K. (1990). The processes of technological innovation, Lexington Books Lexington, MA.

Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A framework for the governance of information security in banking system. Journal of Information Assurance & Cyber Security, 1–12.

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., … others. (2019). Cybercrime case as impact development of communication technology that troubling society. Int. J. Sci. Technol. Res, 8(9), 1224–1228.

Venter, H., and Eloff, J. H. (2003). A taxonomy for information security technologies. Computers & Security, 22(4), 299-307.

Verschuren, P., Doorewaard, H., & Mellion, M. J. (2010). Designing a research project. Eleven International publishing house.

Wagner, C., Kawulich, B., & Garner, M. (2012). Doing social research: A global context. McGrawHill Higher Education.

Wall, D. S. (2015). The Internet as a conduit for criminal activity. Information technology and the criminal justice system. Sage Publications, Inc., 77-98.

Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6th ed.). Cengage Learning.

World Economic Forum. (2018). The Global Risks Report 2018. World Economic Forum, 13th edhttps://www3.weforum.org/docs/WEF_GRR18_Report.pdf

World Economic Forum. (2020). How to protect yourself from cyberattacks when working from home during COVID-19.

World Economic Forum. (2020). Why cybersecurity matters more than ever during the coronavirus pandemic.

Yaseen, Q. (2016). Insider threat in banking systems. doi:10.4018/978-1-5225-0864-9.ch013

Yildirim & Varol. (2019). A Research on Security Vulnerabilities in Online and Mobile Banking.doi: 10.1109/ISDFS.2019.8757495

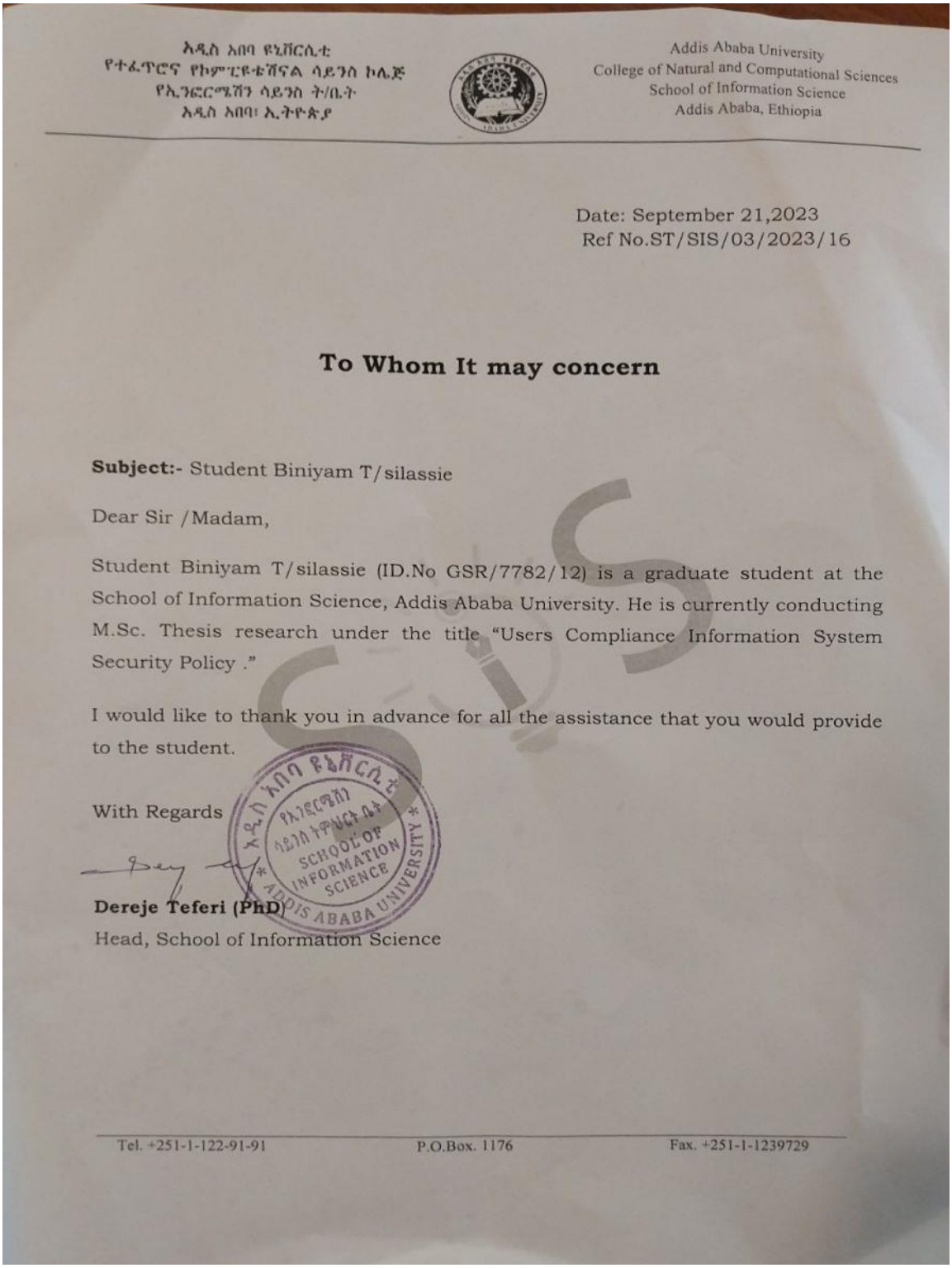
Yin, R. K. (2003). Case study research: Design and methods (2nded.). Newbury Park, CA: Sage.

Yung, C. W., Sun, R., Yenchun, J. W. (2020). Smart city development in Taiwan: From the perspective of the information security policy. Sustainability,12(7),2916. https://doi.org/10.3390/su12072916

ZDNet (2018). Bank web apps are the "most vulnerable" to getting hacked, new research says.

ZDNet (2020). COVID-19 blamed for 238% surge in cyberattacks against banks.

Appendix I: Data Collection Permission Letter



አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮና የኮምፒዩቴሽናል ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት
አዲስ አበባ፣ ኢትዮጵያ

Addis Ababa University
College of Natural and Computational Sciences
School of Information Science
Addis Ababa, Ethiopia

Date: September 21,2023
Ref No.ST/SIS/03/2023/16

To Whom It may concern

Subject:- Student Biniyam T/silassie

Dear Sir /Madam,

Student Biniyam T/silassie (ID.No GSR/7782/12) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting M.Sc. Thesis research under the title "Users Compliance Information System Security Policy ."

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

With Regards

Dereje Teferi (PhD)
Head, School of Information Science

Tel. +251-1-122-91-91 P.O.Box. 1176 Fax. +251-1-1239729

Appendix II: Interview Questions

Questions related to Information security practices at the Ministry of Finance

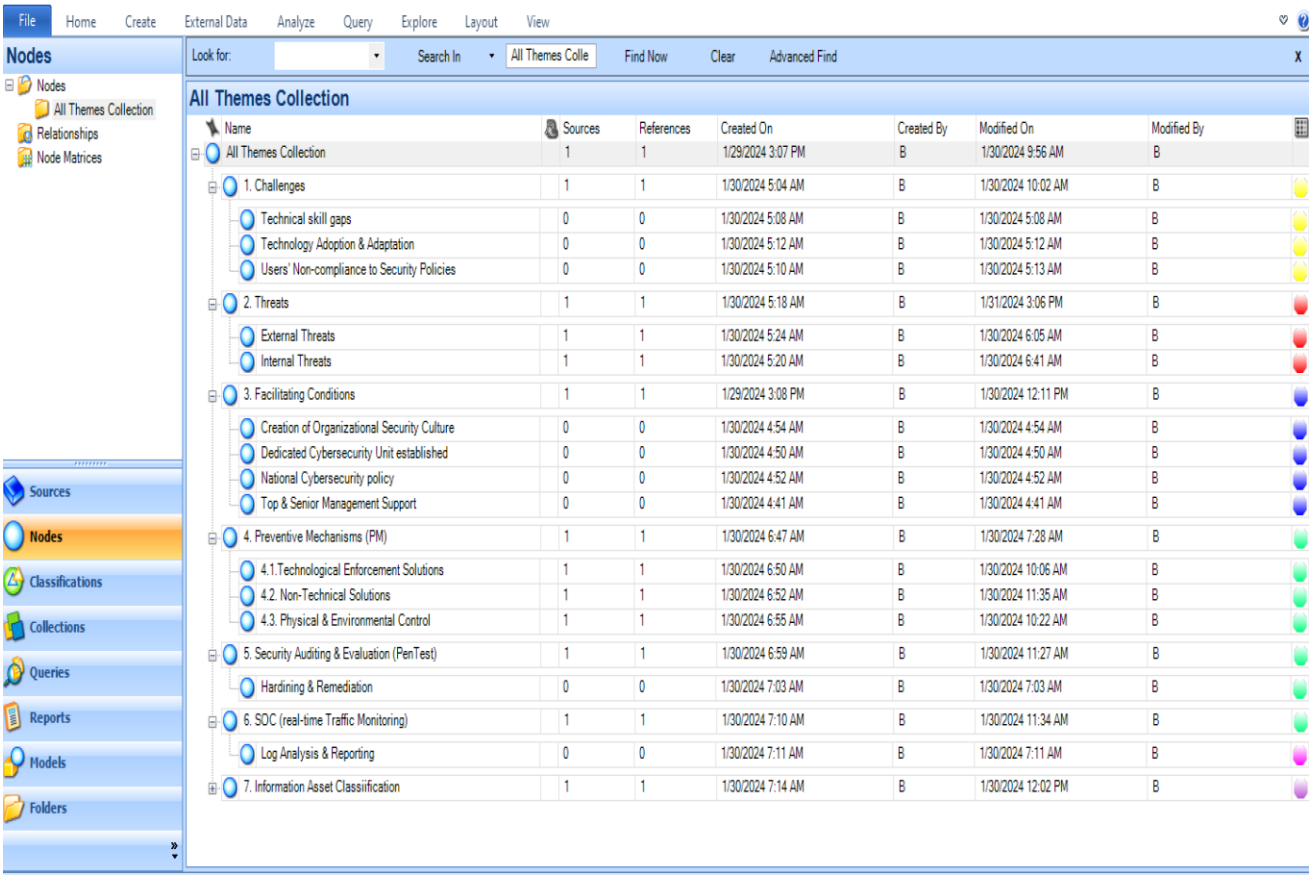
1. what are the main security threats in your organization?
2. What prevention mechanisms have you introduced to protect security threats?
3. Do you have approved security policy document? when it was approved? who developed it?
4. Is your policy document exhaustive (or all-inclusive) and complete? what limitations it has?
5. Does your employees comply to the information security policy?
6. what did you do to make employees to comply to the InfoSec such as
   - 6.1 training?
   - 6.2 top management support?
   - 6.3 employees' attitude to the organization's IT resources safety?
   - 6.4 punishment for those employees who do not comply? what kind of punishment?
   - 6.5 incentives or rewards for those employees who comply? what kind of incentives?
   - 6.6 Any tools or technology enforcement that makes employees to be complying?
7. Do you have any other suggestions to add?

Thank you for your cooperation!

Date: October, 2023 G.C

Appendix III: Data Coding at NVivo software

This is data organization and categorization.



Appendix IV: Information System Security Framework Evaluation Checklist Questions

The purpose of this checklist is to assess the applicability and effectiveness of the developed Information Security framework in order to adopt it and improve information security practices.

1. Has the framework identified and addressed any barriers or challenges that may hinder the implementation of facilitating conditions?

2. Has the framework included challenges and risks faced by the MoF in relation to InfoSec?

3. Has the framework covered all information system security threats faced by the MoF?

4. Does the proposed framework cover all controls and measures that can mitigate the identified threats effectively?

5. Does the framework include provisions for regular security audits and evaluations to assess the effectiveness of the implemented security controls?

6. Has the framework allowed to monitor and respond to information security incidents?

7. Are there specific technical controls, such as firewalls, IDS/IPS, antivirus, AD/DC and NAC preventive mechanisms, outlined within the framework?

8. Do the framework address non-technical controls, such as policies, procedures, and training, to support a holistic approach to information security?

9. Can the framework address physical security aspects, such as access controls and surveillance systems?

10. What is your overall evaluation about the proposed information system security framework?

Appendix V: Proposed Information System Security Framework

The proposed framework comprises six components that interact with each other. Each component serves its unique set of functions.