
**Addis Ababa University**

**Addis Ababa Institute of Technology**

**School of Information, Technology and Engineering (SiTE)**

# Cybersecurity Maturity Assessment Framework:

# The Case of Ethiopian Banks

**A Research Thesis Submitted to the Graduate School of Addis Ababa University in School of Information, Technology and Engineering (SiTE)**

By: **Yafet Ashebir**

Advisor: **Dr. Elefelious Getachew (PhD)**

Addis Ababa, Ethiopia

October 2024

# Cybersecurity Maturity Assessment Framework:

# A Case of Ethiopian Banks

**Name and signature of Members of the Graduate Examining Committee**

| | **Signature** | **Date** |
|---|---|---|
| Dr. Elefelious Getachew (PhD)<br>Research Advisor | _____ | _____ |
| Dr. _____<br>Examiner | _____ | _____ |
| Dr. _____<br>Examiner | _____ | _____ |

October 2024

## Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that the thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor, Dr. Elefelious Getachew (PhD). Other sources are acknowledged by proper citations giving explicit references. A list of references is appended.

Signature: _____

Yafet Ashebir

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

Advisor's Signature: _____

Dr. Elefelious Getachew (PhD)

## Acknowledgment

In this thesis, I am glad to have a great opportunity to thank God and acknowledge the people who helped me throughout the research paper process.

Firstly, I want to thank my research advisor and mentor Dr. Elefelious Getachew (PhD) for his unwavering support starting from the very first stage of this thesis. I believe that I have learned so much from him and pleased by his continuous encouragement. Then, I would like to thank the Graduate Execution Committee: Dr. Henock Mulugeta (PhD), Dr. Sileshi Demisse (PhD), and other GEC members for providing me with *enough time* to conduct my research and encouraging me to add value to the scientific community.

Finally, I would like to thank cybersecurity directors and professionals of the selected banks I got the data from to conduct my research for their support and willingness.

## Abstract

*As the banking sector becomes a key player in globalized cyberspace with increasing reliance on digital services, it is prone to a wide range of emerging cybersecurity risks. As cybersecurity can only be achieved through a well-organized set of controls; existing cybersecurity maturity frameworks, while comprehensive and vague, fail to address the unique cybersecurity challenges faced by Ethiopian banks. The literature review discovered that no study has proposed a cybersecurity maturity assessment framework for the Ethiopian banking sector.*

*This study aims to propose a customized framework by reviewing multiple cybersecurity maturity assessment frameworks to identify their weaknesses and strengths. After a thorough assessment, we have identified the major limitations of the existing frameworks and they are not easy to understand, expensive to implement, require intensive and equipped human resources, and are not tailored to the banking sectors to fix operational challenges. Moreover, to assess existing cybersecurity maturity frameworks in banks, data was collected from 9 selected governmental and private banks, and a thematic analysis approach was utilized for the qualitative data collected. As the findings reveal, all selected banks don't have a proper cybersecurity maturity assessment framework as well as improper adoption of international standards.*

*To address identified weaknesses, a customized cybersecurity maturity assessment framework is proposed to enable banks to identify their security posture and manage their security risks. The proposed framework comprises various components such as regulatory requirements, personal data protection, supply chain security, awareness and culture development, cyber governance, cyber risk management, business continuity and disaster recovery, incident response plan, information sharing, and collaboration, and incorporates international best practices like General Data Protection Regulation (GDPR). To evaluate the framework expert review has been done as the framework contributes to both academic literature and industry practice by providing a customized framework for banks to assess and improve their cybersecurity maturity.*

***Key Words**: Cybersecurity, Cybersecurity Maturity, Cybersecurity Maturity Assessment Framework*

# List of Abbreviations

| | |
|---|---|
| ATM | *Automated Teller System* |
| BEC | *Business Email Compromise* |
| CCSMM | *Community Cyber Security Maturity Model* |
| CERT – RMM | *Computer Emergency Response Team – Resilient Maturity Model* |
| CIS | *Center for Internet Security Controls* |
| CIS RAM | *Center for Internet Security Controls - Risk Assessment Method* |
| COBIT | *Control Objectives for Information and Technology* |
| CMAF | *Cybersecurity Maturity Assessment Framework* |
| CMCSRS | *Critical Mass Cyber Security Requirement Standard* |
| CS | *Cyber Security* |
| C2M2 | *Cybersecurity Capability Maturity Model* |
| CREST | *Council for Registered Ethical Security Testers* |
| DDoS | *Distributed Denial of Service* |
| FSSCC CAT | *Financial Services Sector Coordinating Council* |
| GDPR | *Global Data Protection Regulation* |
| GCSCC | *Global Cyber Security Capacity Center* |
| HITRUST CSF | *Health Information Trust Alliance Common Security Framework* |
| ISO27001:2022 | *International Standard Organization* |
| IT | *Information Technology* |
| ITIL | *Information Technology Infrastructure Library* |
| MITM | *Man-In-The-Middle* |
| NBE | *National Bank of Ethiopia* |
| NICE CSF | *National Initiative for Cybersecurity Education – Cybersecurity Maturity Model* |
| NIST CSF | *National Institute of Standards and Technology - Cyber Security Framework* |
| NIST SP-800 | *National Institute of Standards and Technology – Special Publication* |
| PCI DSS | *Payment Card Industry – Data Security Standard* |
| SSE – CMM | *System Security Engineering – Cybersecurity Maturity Model* |
| USD | *United State Dollar* |
| UK | *United Kingdom* |
| YoY | *Year on Year* |

# Contents

# List of Figures

# List of tables

# Chapter One

## 1. Introduction

This chapter begins with a concise overview of the issues about the significance of cybersecurity and its application in the banking sector of Ethiopia. The subsequent section addresses the research problem, followed by a presentation of the fundamental research questions. This is succeeded by an explanation of the study's motivation. The fifth and sixth sections, respectively, discuss about the objectives, significant contributions, and scope of the research paper. The chapter concludes with an outline of the thesis organization.

### 1.1. Background Information

The cybersecurity landscape is undergoing rapid changes, and the associated threats are no longer novel, as organizations in Ethiopia across various sectors, including government, military, corporate, financial, and healthcare, are amassing and processing vast amounts of data on digital devices. As cyber risks such as network attacks and data breaches increase, businesses in all industries are elevating cybersecurity risks to a high-priority business concern. To achieve effective cybersecurity, organizations must coordinate efforts throughout their entire cyber infrastructure. Security measures are crucial in safeguarding the confidentiality, availability, and integrity of cyber systems by preventing asset losses from cybersecurity attacks. The consequences of cybersecurity failures include the theft of intellectual property, direct financial losses from cybercrime, compromise of sensitive business information, operational sabotage, additional costs for system recovery, and a decline in stakeholder confidence in the system. [1].

A study [2] examining cybercrime in Ethiopia, which surveyed 40 financial institutions, revealed that all participants had encountered various cybercrime incidents. The most common attacks included computer viruses, worms, malware, or other malicious intrusions (57.1%), website defacement (40%), unauthorized access (17.1%), and spam (14.7%). Additionally, computer data breaches (62.9%), denial of service (DOS) attacks (45.7%), and system interference (45.7%) were frequently reported cybercrimes targeting these organizations. The survey findings indicate that cybercrime is a significant issue in Ethiopia. Furthermore, globally, the banking industry alone is the most targeted industry for cyber-attacks due to the amount of financial and personal data it holds as well as its assets. Recent data regarding the attack vector reports [3] showed that phishing accounted for 36% of breaches across all industries with the banking sector as a primary target, [4] The banking sector alone experienced a 1318% YoY increase in ransomware attacks, [5]

indicates banks are the second most targeted areas for DDoS attack behind government organizations, [6] add 47% two-year increment in insider threats in the banking sector, [7] exhibited 51% coverage of third-party attacks targeting banking sector and 118% YoY increment of malware in mobile money apps [8]. Additionally, [9] showcases that ATM skimming, jackpotting, and malware attacks emerged with a 269% rise in 2020.

Given the limited ability of institutions to detect cybercrime, it is reasonable to assume that the actual prevalence of cybercrime in Ethiopia may be higher than what this survey suggests. Organizations have critical assets that are exposed to cyber threats which exploit vulnerabilities that in turn affect confidentiality, integrity, and availability of information. Cybersecurity has become an essential tool for managing security risks. If implemented properly, it creates confidence and trust leading to the success of the business. Several cybersecurity maturity assessment models have been developed and used to mitigate security risks by organizations. According to [10] Research finding definition, cybersecurity maturity assessment helps to identify the readiness level of an organization to protect itself from cyber threats. There is a need to adopt a strategy that should outline the expression of vision, high-level objectives, guiding policy principles, and explicitly accepted priorities by an organization in a bid to address specific cybersecurity issues. Businesses already have controls at their disposal to help them keep their systems and networks safe. This includes cybersecurity models or frameworks to provide a way for measuring and communicating cybersecurity readiness to relevant stakeholders thereby ensuring regulatory compliance and corporate responsibility. An organization's success at achieving a specific goal is evaluated using a maturity model. Additionally, it might make it easier for a company to determine where its procedures are strong and where they are not at all [11] . A cybersecurity maturity model can be used to compare similar companies in an industry as well as track advancements made over time by integrating security into an organization's tactical and strategic workflows. Conducting a cybersecurity maturity assessment for the organization will therefore provide an assurance of the preparedness against cybersecurity threats. With this in place, an organization can identify, assess, prioritize, and mitigate its cybersecurity risks promptly.

This research work proposed a customized Cybersecurity Maturity Assessment Framework (CMAF) that can be used to guide the banking industry to assess the existing cybersecurity maturity level and identify exact security posture.

### 1.2. Motivation of the Study

The motivation for studying a Cybersecurity Maturity Assessment Framework (CMAF) in Ethiopian banks can be understood by considering the increasing importance of information systems security in the face of growing security threats. [12]. Ethiopian banks, as integral components of the nation's financial sector, contribute to macroeconomic stability and growth, making their security a matter of national importance [13]. The current maturity level of information security governance in Ethiopian banks is at level 2, indicating a need for improvement and a more consistent application of security measures [12]. However, existing literature reveals an absence of recent studies on the cybersecurity maturities of Ethiopian banks. First, as a motivation, the lack of in-depth research on this specific area leaves a significant gap in understanding the current state of cybersecurity preparedness in the Ethiopian banking industry. Without this crucial information, it becomes challenging to identify specific vulnerabilities, prioritize security investments, and develop targeted improvement strategies [14] [12].

Secondly, the research is further motivated by the need for sector-specific frameworks that cater to the unique requirements of different industries. For example, these researchers [15] [16] [17] Proposed a cybersecurity maturity framework tailored for medical institutes in prioritizing privacy and personal medical data; presented a holistic maturity framework that considers both local and international security standards to address the gap in higher education; and introduced a holistic cybersecurity maturity assessment framework that incorporates security regulations, data protection, and best practices in higher educations, respectively.

Interestingly, as a third motivation, while there is a recognition of the need for cybersecurity maturity models that integrate various regulations [17], and specific directives, Ethiopian banks may also benefit from a framework that considers both local and international standards (as a best practice), as seen in other contexts [18] [16]. The lack of diversified and international banking services in Ethiopia [19] further underscores the need for a robust cybersecurity framework to support the sector's growth and integration into the global financial system. Finally, another motivation for studying cybersecurity maturity assessment frameworks is driven by the urgent need to provide organizations with comprehensive, adaptable, and sector-specific tools to evaluate and enhance their cybersecurity posture. This framework not only helps in identifying security

gaps but also guides the implementation of improvements, ultimately contributing to a more resilient and secure digital ecosystem across various industries and sectors.

In summary, the motivation for implementing a CMAF in Ethiopian banks is driven by the need to enhance the security of their information systems, align with international best practices, and support the sector's growth and contribution to the national economy. The adoption of such a framework would likely address the identified security gaps and maturity level deficiencies, thereby strengthening the resilience of the banking sector against cyber threats [12].

### 1.3. Problem of the Statement

The Ethiopian banking sector is one of the fastest expanding industries in the country and is quickly experiencing rapid digitalization of its banking operations. Increasingly dependent on the operation of the information systems, the banking sector is likewise investing extensively in digital services and related infrastructure exposing it to an increasing array of cybersecurity threats. The lack of contextualized understanding regarding cyber security maturity is the main obstacle to cybersecurity in the banking business. Because of this, this existing gap hinders the development of effective security approaches to enhance the sector's resilience against cyber-attacks. The research problem, therefore, centers on the need to enable banks to assess and improve the cybersecurity maturity levels to ensure the protection of sensitive financial data and maintain public trust in the digital banking ecosystem [12]. Most of the bank’s focus is on implementing cybersecurity best practices merely to meet the external requirements [20].

A poor evaluation of an organization's cyber maturity level may result in incorrectly set priorities and/or occasionally wasted investment. It is crucial to understand the controls in place as well as the existing security posture [21]. Since there aren't many resources available for investing in cybersecurity, it's important to reduce associated risks as effectively as possible. To reduce these risks, an organization must evaluate its readiness for cybersecurity management by understanding its cybersecurity maturity level, which serves as a gauge of its capacity to recognize and defend information assets against potential cyber-attacks. Organizations should essentially be aware of the cyber threat landscape they confront and should have a clear measurement instrument and path to enhance their cybersecurity maturity assessment. Even though there are cybersecurity maturity models that can be employed, finding trained professionals has been a concern for many when conducting cybersecurity maturity assessments. Contextualization is required because the existing

models might not be simply adopted to cover all important security minimum requirements and government or regulatory body regulations.

Additionally, the unique regulatory environment of Ethiopia adds complexity to the cybersecurity landscape of its banking sector. The rapid adoption of digital banking services, coupled with potential gaps in digital literacy among customers and staff, creates a prolific ground for cyber threats such as phishing, third-party attacks, ransomware, and insider attacks. Understanding how these factors interact with the cybersecurity maturity of Ethiopian banks is crucial for developing effective cyber risk mitigation strategies [22] [14]. The absence of a tailored cybersecurity maturity assessment framework is another critical issue. [12] While other cybersecurity maturity assessments framework exists worldwide, [15] There is a need to have a framework that incorporates Ethiopian-specific regulatory requirements, security context, and the unique challenges faced by the financial sector, especially banks.

This leads to the following problem statement:

*The primary problem this study aims to solve is the lack of a tailored cybersecurity maturity assessment framework (CMAF) that addresses the unique regulatory and operational cybersecurity challenges faced by Ethiopian banks. The lack of such a customized framework leaves the Ethiopian banking industry exposed to advanced cyber threats that can exploit existing security weaknesses. This vulnerability not only puts banks at risk of financial and reputational harm but also hinders their ability to adhere to national and industry-specific regulations and effectively manage security incident.*

This research proposes a cybersecurity maturity assessment framework (CMAF) that is specifically designed for the Ethiopian banking sector. The proposed solution will help banks systematically assess their cybersecurity posture, identify gaps, and implement targeted improvements tailored to their unique operational and regulatory contexts.

### 1.4. Research Questions

The study intended to address the following research questions:

- ***RQ1****: What available cybersecurity maturity assessment frameworks do Ethiopian banks use to assess their cybersecurity?*

- ***RQ2****: What are the positive aspects and limitations of existing cybersecurity maturity assessment frameworks, and how applicable are they in Ethiopian banks?*

- *RQ3: What innovative and customized solution be tailored to address the specific needs and challenges of the Ethiopian banking sector while incorporating the best practices of existing cybersecurity maturity frameworks?*

- *RQ4: What metrics or mechanisms can be used to measure the effectiveness of the proposed framework in achieving its intended outcomes?*

## 1.5. Objective of the Thesis Study

### 1.5.1 General Objective

The general objective of this research work is to develop and evaluate a customized cybersecurity maturity assessment framework tailored to the specific needs and challenges of Ethiopian banks.

### 1.5.2 Specific Objectives

The specific objective of the research work includes:

- Assess existing practices and identify available cybersecurity maturity assessment frameworks (CMAF) used in Ethiopian banks,

- Conduct a comprehensive literature review and industry analysis to identify all available cybersecurity maturity assessment frameworks (CMAF) related to banks,

- Identify and categorize peculiar features and parameters that are important for the Ethiopian context,

- Propose a contextualized and customized cybersecurity maturity assessment framework to address the specific needs and challenges of the Ethiopian banking sector,

- Analyze the effectiveness of contextualized and customized cybersecurity maturity assessment frameworks (CMAF) in accurately measuring the cybersecurity posture/maturity of Ethiopian banks.

## 1.5. Contribution of the Thesis Study

This research work provides the following contributions:

- It provides a contextualized and customized framework, enabling the banking industry to utilize a shared assessment framework tailored to their specific requirements and constraints,
- It possesses the capability to identify the cybersecurity posture of Ethiopian banks by effectively assessing their current cybersecurity state and guiding them toward a desired state,
- The framework introduces crucial components such as awareness and culture development, personal data protection, supply chain security, mobile money security, ATM security, information sharing and collaboration, and regulatory compliance, respectively,
- The personal data protection component will enable banks to gain trust from their customers as it will prove transparency on data being processed,
- It enables Ethiopian banks to benchmark against peer local and international banks, identifying areas for improvement and driving continuous enhancement.
- A comprehensive analysis of existing cybersecurity maturity assessment frameworks has been conducted, and their limitations are discussed,
- It addresses the scarcity of information regarding cybersecurity maturity in Ethiopia, creating an opportunity for further in-depth research in this field of study and enhancing the proposed framework,
- It has the potential to motivate and aid policymakers and regulatory bodies to design, develop, and enforce effective cybersecurity maturity assessment frameworks at the national level,
- The proposed framework promotes an industry-specific approach to address industry-specific cybersecurity needs and challenges,
- The proposed framework can be seen either as a benchmark or be adapted and expanded for application in other sectors within Ethiopia. Additionally, it provides a blueprint for emerging markets like FinTech as cyber threats related to financial activities rely on new technologies.

### 1.6. Scope and Limitation

The research scope of this study is limited to assessing and proposing the maturity assessment framework for selected banks in Addis Ababa, Ethiopia. As a sample, nine banks were selected

for the study. Due to time and resource constraints, we are limited to narrow the focus of the research on the HQs of the selected banks.

### 1.7. Organization of the Document

This research paper is organized into seven chapters. chapter one discusses the background of the study, motivation of the study, the statement of the problem, the research questions, the research objectives, the scope of the research, and the expected output of the study would provide contribute to the financial sector are discussed in contribution of the study sub tittle. Chapter two discus the literature review in cybersecurity, cybersecurity maturity, and related disciplines. In this chapter trending cyber threats, cybersecurity maturity frameworks, and related works are reviewed and presented. Chapter three provides the detail description about the research design and methodology implemented. Under this section, the research design, the research technique, and ethical considerations are presented. Chapter four explicitly discuss the proposed cybersecurity maturity assessment framework alongside with the validation mechanics. Chapter five deals with the data analysis. Chapter six focuses on findings and discussion. The final chapter, chapter seven is the final portion for this paper as it gives overall conclusion and recommendation to banks to utilize the proposed framework to identify their existing cybersecurity posture and manage cyber risks. Additionally, it invites researchers to address issue that was not included in this research scope.

# Chapter Two
# 2. Literature Review and Related Works

## 2.1. Literature review

The purpose of this chapter is to review literatures and related works that has occurred thus far, as well as the theoretical and related literature, to provide an understanding of the level of cybersecurity maturity frameworks/models. The review is based on a thorough reading of a specific body of references relating to cybersecurity maturity and its applicability. Thus, this chapter addressed the following important topics: cybersecurity, trending cyber threats, cybersecurity maturity, cybersecurity maturity frameworks, cybersecurity maturity assessment frameworks in the financial sector, overview of cybersecurity maturity frameworks, comparison of existing cybersecurity maturity assessment frameworks, and summary of related works.

### 2.1.1 Cybersecurity

The term "cybersecurity" has been widely studied in academic and popular literature, frequently from a particular perspective. The phrase is used widely [26] with definitions that are extremely varied, context-dependent, usually subjective, and occasionally devoid of useful information. The exact meaning of the term and how it is used in different settings are not well understood. Insufficient clarity regarding a concise, universally recognized definition that considers the complexity of cybersecurity could impede advancements in science and technology by solidifying the primarily technical understanding of cybersecurity and dividing fields that ought to be working together to tackle intricate cybersecurity problems.

Cybersecurity is “the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this” [23]. Hence, others [24] Propose a detailed overview of cybersecurity as the organization and collection of tools, procedures, and structures used to safeguard electronic networks and systems that can access them against situations where de jure and de facto property rights. Information has evolved into the most precious asset to safeguard from insiders, outsiders, and competitors, and cyber security has become a key component of modern banking in our society today [25]. The way the institutions in the banking sector process and store data has changed significantly as a result of the deployment of information technology. [26] This industry is now prepared to deal with a variety of changes, including e-money, e-cheques, e-commerce, internet banking, mobile banking, and other cutting-edge ways of providing services

to clients. Consumers are, nevertheless, highly concerned about identity theft and privacy. Security is viewed as the most important requirement by business partners, suppliers, and vendors, especially when offering shared network and data access. To ensure safe operations, which are attained through the application of cybersecurity best practices, it is therefore a discipline that involves technology, people, information, and procedures [27].

Concern over cybersecurity is spreading quickly to several industries, including the chemical, defense, intelligence, and financial sectors. Given the possible dire implications, dealing with cybersecurity vulnerabilities is a complex and essential undertaking given the growing reliance on networked critical devices [28]. Due to competing operational objectives and overwhelming working environment, cybersecurity threats in the financial industry are improperly managed, even though they pose a serious threat to customer data privacy and security [29].

### 2.1.2 Cybersecurity Threats

An organization's information asset needs to be shielded from risks to information security. Any circumstance or event that has the potential to harm an information system by erasing, destroying, altering, or revealing data, or by refusing service, is considered a danger to an information asset [30]. Information security flaws can corrupt or steal data from a system within an organization or from the organization. Furthermore, a security incident is an occurrence that leads to a breach in data or a network. These kinds of system breaches or damages occur when threats take advantage of holes in the information system.

The banking sector has increasingly become a primary target for cybersecurity threats, as financial institutions hold vast amounts of sensitive data, process large volumes of financial transactions, and operate within a critical infrastructure that is vital to national and global economies. The rise of digital banking, mobile banking services, and online financial platforms has further exposed the sector to a wide array of sophisticated cyber-attacks [31]. These threats are multifaceted and continuously evolving, impacting not only the financial stability of institutions but also customer trust and regulatory compliance. Out of multiple financial sector cyber threats, the following points are quite vital to mention.

#### *2.1.2.1 Phishing*

One of the most prevalent cybersecurity threats in the banking sector is phishing, where attackers attempt to trick users into providing sensitive information, such as login credentials or account

details. Phishing attacks often take the form of deceptive emails or websites designed to mimic legitimate financial institutions. [32] phishing is responsible for a significant portion of data breaches in the financial sector, as banks rely heavily on customer-facing services, making their users vulnerable to social engineering attacks. "Additionally, Business Email Compromise (BEC), a more targeted form of phishing, has also increased, where attackers impersonate a senior executive or vendor to trick employees into transferring funds or sharing sensitive data" [33].

#### *2.1.2.2 Ransomware*

Another major threat facing the banking sector is ransomware, a type of malware that encrypts an institution's data and demands payment for its release. In recent years, ransomware attacks on banks have grown in sophistication, with attackers using advanced encryption methods and targeting core financial systems. The disruption caused by such attacks can result in significant financial losses, reputational damage, and operational paralysis. [34] financial institutions continue to be a top target for ransomware groups, with attacks frequently designed to exploit vulnerabilities in legacy systems or unpatched software.

#### *2.1.2.3 DDoS*

Distributed Denial of Service (DDoS) attacks also pose a serious threat to banks. These attacks involve overwhelming a bank's online services or network infrastructure with excessive traffic, causing disruption or downtime. DDoS attacks can be particularly damaging for financial institutions, as they can cripple online banking platforms, ATMs, and payment systems, leading to significant service outages and financial losses. [35] highlights that many banks have become frequent targets of such attacks, often used as a distraction to mask other forms of cybercrime, such as data breaches or fraud.

#### *2.1.2.4 Insider threats*

Insider threats are another critical cybersecurity risk in the banking sector. Insider threats can originate from current or former employees, contractors, or partners who have access to a bank's systems and data. [36] found that in the Ethiopian banking sector, insider threats are often underestimated, despite the significant risk they pose. Disgruntled employees or those with financial motivations can misuse their access to commit fraud, steal sensitive data, or sabotage systems. [37] research also underscores the growing impact of insider threats, noting that they are often more difficult to detect and mitigate compared to external cyber-attacks, as insiders typically have legitimate access to critical systems.

#### *2.1.2.5 Third-party attacks*

The growing reliance on third-party vendors in banking operations has also introduced new cybersecurity risks. Banks frequently outsource services such as payment processing, cloud storage, and IT support to external providers. However, these third-party relationships can expose banks to supply chain attacks, where hackers compromise a vendor's system to gain access to the bank's network. [1] points out that the increasing interconnectedness of banks with third-party vendors has created new vulnerabilities, especially as many vendors may not adhere to the same stringent security protocols as the banks they serve.

#### *2.1.2.6 Mobile Money attacks*

Moreover, the shift towards mobile banking and fintech platforms has opened up additional attack vectors for cybercriminals. Mobile banking apps, while convenient for customers, are often susceptible to malware, man-in-the-middle (MITM) attacks, and session hijacking. Attackers exploit vulnerabilities in the app's code or operating system, intercepting communication between the user and the bank. [12] emphasized that in the Ethiopian context, the security hygiene practices of mobile banking users and employees are often insufficient, making mobile banking services a lucrative target for cyber-attacks. This is exacerbated by the fact that many mobile devices are not adequately protected with strong encryption or up-to-date security patches.

#### *2.1.2.7 ATM Attacks*

Additionally, ATM attacks have persisted as a threat, particularly through skimming devices that capture card details and PINs. While many banks have adopted EMV chip technology to enhance card security, ATM attacks continue to evolve, with cybercriminals increasingly using malware to manipulate ATM systems directly and extract funds. [38] reported that the Ethiopian banking industry has experienced a rise in ATM fraud, largely due to outdated ATM security protocols and insufficient monitoring. Incorporating ATM security into a cybersecurity framework is particularly crucial for banking institutions operating in emerging economies, where ATMs play a vital role in providing financial services to underserved populations. In nations like Ethiopia, where cash transactions remain common, ATMs are heavily utilized, making them high-value targets for attackers [39].

#### *2.1.2.8 Non-compliance with regulatory frameworks*

Lastly, regulatory pressure and compliance risks also create cybersecurity challenges for banks. Financial institutions are subject to stringent regulations like GDPR and PCI DSS which require

them to protect customer data, ensure privacy, and maintain operational resilience. Failure to comply with these regulations can result in severe financial penalties and reputational damage. [40] highlighted that Ethiopian banks often struggle with the implementation of robust information security policies, partly due to insufficient regulatory frameworks, which further heightens their exposure to cybersecurity threats.

In conclusion, the cybersecurity landscape for banks is constantly evolving, with threats becoming more sophisticated and diverse. As banks continue to digitize their services, they must contend with a wide range of cyber-attacks, including phishing, ransomware, DDoS, insider threats, and third-party vulnerabilities. Addressing these threats requires not only investment in technology but also a focus on staff training, regulatory compliance, and third-party risk management to protect against the financial and reputational risks posed by cybercriminals.

### 2.1.3 Cybersecurity Maturity

[41] For organizations can improve their cybersecurity practices, the industry and the technical community have developed cybersecurity capability maturity models that allow them to measure the cybersecurity capabilities of organizations and position them at different levels. There are different cybersecurity capability maturity models developed by the industry, in many cases developed by state entities to be national/international standards. Therefore, organizations have decided to develop maturity models of cybersecurity capabilities that respond to their needs. Cybersecurity maturity models are widely used to measure an organization's readiness and capability to address cyber threats. These models typically consist of similar elements such as maturity levels and processes, but they often lack a robust validation process [42]. The Global Cyber Security Capacity Centre (GCSCC) has conducted reviews of cybersecurity capacity maturity in various countries, including Lithuania and Samoa, to help governments benchmark their capabilities and prioritize strategic investments [43] [44].

Interestingly, while many cybersecurity maturity models have been proposed in recent years, there is a notable gap in the literature regarding the assessment of these programs. Only a handful of papers and maturity models focus on evaluating the effectiveness of information security and cybersecurity user awareness and training programs [45]. This suggests a need for more research in this area, especially as organizations increasingly rely on these programs to combat cyber-attacks.

The field of cybersecurity maturity assessment is still evolving, with new models being developed to address specific needs. For instance, a Holistic Cybersecurity Maturity Assessment Framework has been proposed for Higher Education Institutes in the United Kingdom, integrating various security regulations and best practices [17]. However, the prevalence of ISO/IEC 27001/27002 standards and the need for further investigation into ISO 21827 highlight the ongoing challenges in establishing a universally accepted approach to cybersecurity maturity evaluation [21]. As cyber threats continue to evolve, there is a growing need for more comprehensive and validated maturity models that can effectively guide organizations in improving their cybersecurity posture.

### 2.1.4 Cybersecurity Maturity Frameworks in Financial Sectors

[46] The banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. Many private banks have been established in the past few years. The distribution and diversity of services is widening. Banking business competition has stirred the advancement of services enabled by information technology. More banks in Ethiopia are implementing Core banking solutions to provide banking services from any of their branch offices. Though this technological advancement has facilitated business processes, much attention should be drawn to thwarting the illegal financial gain efforts of cybercriminals.

To gain sustainable competitive advantage, financial sectors have incorporated information systems and related technology. In today's world, successful activity regulation and good organization approaches are linked to information quality management and monitoring. Financial industries are directly influenced by their reliance on information and technology services, processes, and the underlying mechanisms that form the foundation for these technologies due to the aspect of readily available information [47].

Information security for the financial sector is a part of the information security model that is primarily applicable to the factors that impact information systems, such as data security and all other aspects of the framework. [47]. Information security for financial security is the protection of information assets from unauthorized access, use, alteration, destruction, and deletion. The fast development of information technology allows people to access their mobile phones to conduct business. The underlying major obstacle in the advancement of information technology is that hackers can obtain information in the middle of a communications channel. [48] Hackers are individuals who commit data misinterpretation and data theft. As a result, weak financial

information protection on web servers and technological devices creates vulnerability, which is then exploited by hackers.

The security of the banking information systems and critical financial data should be ensured. The banking sector is more sensitive to the issue of security as money is at stake and is a lucrative target for malicious attackers. Cybersecurity maturity frameworks play a crucial role in the financial sector, as organizations aim to mitigate cyber risks and protect sensitive data. In the financial sector, cybersecurity maturity frameworks are essential for assessing and improving cybersecurity practices. [49] proposed a cybersecurity maturity model specifically tailored for organizations in the financial sector, supported by a measurement tool for diagnosis and result visualization [50] This model can help financial institutions enhance their cybersecurity posture and better protect against cyber threats. Furthermore, [51] surveyed cybersecurity risk management frameworks adopted by organizations to address cyber risks. Overall, cybersecurity maturity frameworks are essential for the financial sector to assess, improve, and maintain cybersecurity practices. Collaborating with regulators, law enforcement, and national cybersecurity agencies can further strengthen cybersecurity defenses in the financial sector [20] By leveraging innovative technologies like blockchain and adopting comprehensive cybersecurity risk management frameworks, financial institutions can enhance their cybersecurity posture and protect against evolving cyber threats.

### 2.1.5 Overview of Existing Cybersecurity Maturity Frameworks

There are plenty of cybersecurity models that have been developed based on the needs of different organizations. The most comprehensive and known models are currently incorporated into international standards [12].

#### 2.1.5.1 General Cybersecurity Maturity Frameworks

*ISO/IEC 27001:2022*

The ISO/IEC 27001:2022 standard is one of the most recognized global standards for Information Security Management Systems (ISMS) [52]. Its main goal is to help organizations systematically manage sensitive information and ensure the confidentiality, integrity, and availability of data by applying risk management processes. This standard is applicable across all industries and sectors and is widely adopted by organizations that handle sensitive information. ISO/IEC 27001:2022 sets out the requirements for establishing, implementing, maintaining, and continually improving ISMS. It follows a process-based approach to initiate, implement, operate, monitor, review, and

improve an organization's ISMS. Organizations are also required to conduct risk assessments and develop policies that address specific threats. This standard is particularly valued for its broad applicability and is widely used by industries that handle regulated data, such as financial services, healthcare, and telecom. However, ISO 27001 is a certification-based model, meaning that organizations can become certified to demonstrate their compliance, which assures clients and partners about their security posture [53].

### *NIST Cybersecurity Framework (CSF)*

The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework that comprehensively suffices and provides a structure for organizations to identify, assess and review their current security risk and posture. The framework conceptualizes and depicts cybersecurity as five maturity levels consisting of Initial, repeatable, defined, managed, and optimized [54]. Additionally, the framework provided a means for evaluating maturity levels after which an organization could potentially set informed and knowledgeable decisions about scalable future investments and essential improvements.


*Figure 1 - NIST CSF and its Categories*

### *COBIT Capability Maturity Model*

The Control Objectives for Information and Technology (COBIT) provide a subtle best practice for Information Technology management. The COBIT assessment model was designed to provide

organizations with a methodology for reviewing the capability of information technology processes [50]. The framework defined six levels of maturity that include:

- ***Incomplete***: at this level, a process that has not been implemented or has failed to achieve the intended purpose,
- ***Performed***: at this second maturity level, a process that has been implemented and achieves the intended purpose,
- ***Managed***: at managed level, a process that has results specified and therefore managed,
- ***Established***: a process that has been well defined and used throughout the organization,
- ***Predictable***: a process that is consistently executed within defined limits,
- ***Optimization***: and at final level, a process that is continuously improved to meet relevant business goals

Based on specific attributes, the COBIT measurement methodology evaluates the degree of achievement for a given process. Process performance, performance management, work product management, process definition, process deployment, process measurement, process control, process innovation, and continuous optimization are a few of the characteristics a process could have.

COBIT also defined evaluation indicators in the measurement framework to identify the process maturity. These indicators include generic practice, which refers to generic-type actions, generic resources, which refers to resources that help achieve the attributes, and generic product, which refers to the collections of traits that are anticipated to emerge as a result of accomplishing an attribute. By doing more performance assessments based on the indicators, the indicators are improved even further.

### *CIS Controls*

The Center for Internet Security Controls (CIS) is a set of cybersecurity best practices designed to help organizations protect against prevalent and dangerous cyber-attacks. [55] Initially introduced as the SANS Top 20, CIS Controls have since evolved to become a set of 18 prioritized actions (as of version 8) that organizations can take to secure their environments. CIS Controls were grouped into three categories:

- Basic Controls: Essential steps for effective cyber hygiene.
- Foundational Controls: Strengthen protection against sophisticated threats.
- Organizational Controls: Focus on people, processes, and the governance of cybersecurity activities.

The framework provides practical and actionable steps for organizations of all sizes and across all sectors. It is risk-based and adaptable, meaning that even smaller organizations with limited resources can adopt controls incrementally. CIS Controls are often used in conjunction with other frameworks, such as NIST CSF or ISO/IEC 27001, and many organizations use it as a stepping stone toward broader compliance efforts.


*Figure 2 - CIS Controls*

### *NIST SP-800 Series*

The NIST Special Publication 800 (SP-800) series is a comprehensive set of guidelines, technical specifications, and recommendations developed by the National Institute of Standards and Technology (NIST) to guide information security. The most widely referenced document in this series is NIST SP 800-53, which provides a catalog of security and privacy controls for federal

information systems and organizations. [56] It emphasizes the risk management framework (RMF), which provides a structured and systematic process for managing information security risks. This approach is particularly valuable in industries such as the government and critical infrastructure sectors, where a high degree of control over security is needed. The framework was designed to be flexible and scalable, making it suitable for organizations of all sizes. NIST SP-800 also includes publications like SP 800-37, which guides risk management for federal information systems, and SP 800-171, which provides cybersecurity controls specifically for non-federal organizations that handle controlled unclassified information (CUI).

### *CIS RAM*

The CIS Risk Assessment Method (CIS RAM) is a cybersecurity framework that integrates CIS Controls with a risk assessment methodology to help organizations assess and manage their cybersecurity risks. CIS RAM allows organizations to evaluate their security controls in the context of specific threats and vulnerabilities, providing a way to measure the effectiveness of their security programs. [57] risk assessment process is based on business priorities and allows organizations to prioritize their efforts to protect the most valuable assets. It is particularly useful for organizations that want to apply CIS Controls in a risk-management context, giving them a structured way to assess their risk and take appropriate actions. Although CIS RAM is highly customizable and flexible, it requires significant internal expertise in risk management to be effectively implemented, which can be a barrier for smaller organizations.

### *CERT Resilience Maturity Model (CERT - RMM)*

This model defined practices for operational resilience, security, and business continuity. It also defined twenty-six process areas categorized into four domains that are engineering, operations, enterprise management, and process management [58]. CERT-RMM also can be used by organizations to chart a structured improvement path by setting improvement targets, measuring current capabilities, and developing improvement plans focused on making mission-critical assets and services more resilient. And, [59] is designed to make more efficient and effective use of domain-specific practices that an organization already uses today rather than replace them.

### *System Security Engineering Capability Maturity Model (SSE - CMM)*

The Systems Security Engineering Capability Maturity Model (SSE-CMM) was developed to advance security engineering as a defined, mature, and measurable discipline. The SSE–CMM

contains processes comprising of Administer Security Controls, assessing impact, Assess Security risks, assessing Threats, Assess Vulnerability, Build Assurance Arguments, Coordinate Security, monitoring system Security Posture, Provide Security Input, Specify Security Needs, and Verify and Validate Security. [60] mentioned the five Capability Maturity Levels that represent increasing process maturity are:

- ***Performed Informally***: at this level, baseline processes are performed,
- ***Planned and Tracked***: at the second level, Project-level definition, planning, and performance verification issues are addressed,
- ***Well-Defined***: the focus is on defining and refining a standard practice and coordinating it across the organization,
- ***Quantitatively Controlled***: this level focuses on establishing measurable quality goals and objectively managing their performance,
- ***Continuously Improving***: at this level, organizational capability and process effectiveness are improved.

### *ITIL*

The Information Technology Infrastructure Library (ITIL) is a framework designed to help organizations manage IT services effectively. [61] Although ITIL is not a cybersecurity framework, it plays an essential role in managing IT security by aligning IT services with business needs, optimizing processes, and improving service management. ITIL focuses on service management best practices to ensure the delivery of reliable and secure IT services. ITIL's service management lifecycle of ITIL covers areas such as service design, service transition, service operation, and continual service improvement. Organizations use ITIL to build a culture of continuous improvement, which helps enhance both their IT and security processes over time. ITIL can be integrated with cybersecurity frameworks such as ISO/IEC 27001 and NIST CSF to enhance the security and reliability of IT services.

### *NICE Capability Maturity Model (NICE - CMM)*

This model was developed by the National Initiative for Cybersecurity Education (NICE) to assist institutions in applying best practices [62]. The National Initiative for Cybersecurity Education Cybersecurity Maturity Model (NICE – CMM) defines three main domains comprising of:

- ***Process and Analytics***: this process represented activities that were associated with the actual steps an organization would take to carry out workforce planning and how they were integrated with other important processes. The Analytics represented activities that were associated with supply and demand data and the use of tools, models, and methods to carry out workforce planning analysis,
- ***Integrated Governance***: the second process represented activities that were associated with establishing governance structures, guidance provision and development, and driving decision making,
- ***Skilled Practitioner and Enabling technology***: the skilled practitioners represented activities that were associated with establishing workforce planners. Enabling technology represented activities that were associated with the accessibility and use of data systems.

Moreover, the framework defined three maturity levels as:

- Limited,
- Progressive, and
- Optimizing.

### *CREST Maturity Assessment Model*

The CREST (an international accreditation and certification body that represents and supports the technical information security market) framework was developed as a tool that could be used to perform maturity-level assessments. These tools were represented in a spreadsheet manner that could be easily used. The tools include:

- A cyber threat intelligence maturity assessment tool that provides a way to conduct a maturity assessment to determine the level attained by organizations in terms of cyber threat intelligence,
- A cybersecurity incident response maturity assessment tool that assesses the status of an organization's cyber incident response capability,
- A penetration testing maturity assessment tool that helps to assess the status of a penetration testing program for an organization.

The CREST [63] assessment tool defined five maturity levels that included: foundation, merging, established, dynamic and optimized.

*Community Cyber Security Maturity Model (CCSMM)*

The Community Cyber Security Maturity Model (CCSMM) [64] was developed to fill this hole and to address the needs of states and communities to develop a viable and sustainable cyber security program. The model provides three important mechanisms needed by communities: a "yardstick" for officials to determine the community's current cyber security posture and level of maturity, a "roadmap" to help them in improving the community's cyber security posture, and a common point of reference and common terminology for individuals in different states and communities to share experiences and lessons learned with each other.

The framework has five maturity levels as:

- Initial,
- Advanced,
- Self-assessed,
- Integrated, and
- Vanguard.

#### 2.1.5.2 Sector-Specific Cybersecurity Maturity Frameworks

*Cybersecurity Capability Maturity Model (C2M2)*

The Cybersecurity Capability Maturity Model (C2M2) model was developed by the US Department of Energy to evaluate and improve cybersecurity in the electricity sector. It provided a framework for improving the cybersecurity posture of organizations of all sizes. [65] focused on assets in use for information technology, operational technology, and the environments in which they operate. This model defined ten domains that had a set of cybersecurity practices. These domains comprise risk management, asset, change and configuration management, identity and access management, threat and vulnerability management, situational awareness, event and incident response, supply chain and external dependencies management, workforce management, cybersecurity architecture, and cybersecurity program management. Additionally, the framework

defined four maturity levels i.e., Maturity Indicator Level 0 (MIL0), Maturity Indicator Level 1 (MIL1), Maturity Indicator Level 2 (MIL2), and Maturity Indicator Level 1 (MIL3).

### *HITRUST CSF*

The Health Information Trust Alliance Common Security Framework (HITRUST CSF) is a certifiable framework that integrates several global standards, including ISO/IEC 27001, NIST, HIPAA, and PCI DSS, to provide a comprehensive approach to managing risk in highly regulated industries, particularly healthcare. [66] is designed to be scalable based on the size, complexity, and regulatory needs of an organization. It focuses on managing privacy, cybersecurity, and regulatory compliance, using a unified approach. This framework is used by many healthcare organizations to ensure compliance with the HIPAA and other regulations. One of the strengths of the HITRUST CSF is its prescriptive approach, which helps organizations implement detailed security controls while simultaneously meeting the requirements of multiple regulations. The framework also offers certification, giving organizations a way to demonstrate compliance across multiple standards and laws.

### *PCI DSS*

The Payment Card Industry Data Security Standard (PCI DSS) was developed by the Payment Card Industry Security Standards Council (PCI SSC) to secure credit card transactions and protect cardholder data. This standard applies to any organization that processes, stores or transmits credit card data, making it essential for the financial, e-commerce, and retail industries. [67] is a compliance-focused standard with 12 high-level requirements, including measures for encryption, firewalls, vulnerability management, authentication, and access control. Compliance with PCI DSS is mandatory for organizations that handle cardholder data, and noncompliance can result in hefty fines, penalties, or loss of business relationships with credit card providers. One of the key challenges of PCI DSS is that the standard is updated regularly to address emerging threats, requiring organizations to continuously assess and improve their security postures.

### *FSSCC Cybersecurity Profile (Financial Services Sector Coordinating Council)*

The Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile was introduced as a scalable cybersecurity framework tailored specifically for the financial services industry. Developed in collaboration with key U.S. financial regulatory bodies, including the Federal Reserve and the Office of the Comptroller of the Currency (OCC), the profile offers

financial institutions a way to streamline their cybersecurity risk management and regulatory compliance efforts [68].

One of the key features of the FSSCC Profile is its risk-based approach. It helps institutions align their cybersecurity practices with their inherent risk and business complexity. The framework provides a tool that integrates several existing regulatory and cybersecurity frameworks, including the NIST Cybersecurity Framework (NIST CSF), the Gramm-Leach-Bliley Act (GLBA), and the European Union General Data Protection Regulation (GDPR**)**. By offering a unified approach, the FSSCC Profile allows financial institutions to assess their cybersecurity posture and ensure compliance with multiple regulatory frameworks simultaneously.

However, the FSSCC Profile is not without limitations. While it provides extensive guidance for larger, more complex organizations, some critics have noted that small and medium-sized financial institutions may find it too complex or resource-intensive to implement effectively [69]. In addition, while the profile is intended to be global in scope, it is heavily aligned with U.S. regulatory requirements, potentially limiting its direct applicability to institutions outside the U.S.

### *FFIEC CAT (Federal Financial Institutions Examination Council Cybersecurity Assessment Tool)*

The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) was developed to help financial institutions identify their risks and assess their cybersecurity preparedness. The tool was introduced in 2015, in response to increasing regulatory scrutiny and cyber threats targeting the financial services industry. The FFIEC CAT is structured to assess an institution's cybersecurity maturity across five domains: Cyber Risk Management and Oversight, Threat Intelligence and Collaboration, Cybersecurity Controls, External Dependency Management, and Cyber Incident Management and Resilience [70].

The FFIEC CAT provides financial institutions with a comprehensive means to evaluate their cybersecurity risks, offering a detailed assessment of both inherent risk and maturity. Inherent risk is assessed based on factors such as the institution's size, technology, and customer base, while maturity levels range from baseline to innovative, depending on the strength of the institution's cybersecurity controls and governance.

One key advantage of the FFIEC CAT is its structured, step-by-step approach to assessing cybersecurity preparedness, making it accessible for institutions of various sizes. Financial institutions use the tool to benchmark their cybersecurity maturity and identify gaps in their security practices [71].

However, despite its strengths, the FFIEC CAT has faced criticism for being resource-intensive, especially for smaller financial institutions. While the tool provides thorough guidance, smaller institutions may lack the resources to conduct a comprehensive assessment without outside assistance [72]. Additionally, the tool's focus on inherent risk sometimes leaves smaller institutions with limited options for reducing risk beyond enhancing their control environments.

### 2.1.8 Comparison of Existing Cybersecurity Maturity Frameworks

| ***Models*** | ***Function*** | ***Applicability*** | ***Focus*** | ***Cyber-centric*** | ***Implementation*** | ***Time*** | ***Cost*** | ***Required Expertise*** | ***Certification*** | ***Need for Custom*** |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO27001 | *Guidelines for establishing, implementing, maintaining, and improving an (ISMS)* | *Applicable to all industries* | *Information security management, risk management, and protection of information assets* | *Yes* | *Require high resource commitment* | *6 to 12 months* | *Very high cost* | *Highly Required* | *Certification required* | *Moderate* |
| NIST CSF | *Guides organizations in identifying, protecting, detecting, responding, and recovering from cybersecurity threats* | *Applicable to all industries* | *Risk management, cybersecurity governance, incident response, and recovery* | *Yes* | *Lack of specific implementation details* | *4 to 8 months* | *Medium cost* | *Highly Required* | *No formal certification required* | *Moderate* |
| COBIT 5 | *Govern and manage IT enterprise governance, focusing on the integration of IT strategy with business goals* | *Applicable to all industries* | *IT governance, aligning IT strategy with business objectives, risk management, and regulatory compliance* | *No* | *Complexity in implementation and maintenance* | *6 to 12 months* | *High cost* | *Required* | *Certification required* | *Moderate* |
| C2M2 | *Focuses on improving cybersecurity capabilities for critical infrastructure sectors* | *Primarily for critical infrastructure* | *Cybersecurity maturity, capability improvement, and resilience for critical infrastructure* | *Yes* | *Typically implemented by critical infrastructure sectors.* | *4 to 6 months* | *High cost* | *Required* | *No formal certification required* | *Moderate* |
| CIS CONTROL | *A prioritized set of actions or best practices against cyber threats* | *Applicable to all industries* | *Security controls and best practices* | *Yes* | *Focuses primarily on technical controls* | *3 to 6 months* | *High cost* | *Highly Required* | *Certification required* | *Moderate)* |
| NIST SP-800 | *Security standards and guidelines for implementing, managing, and securing IT system* | *Applicable to all industries* | *Security controls and guidelines for IT systems, risk management, and compliance* | *Yes* | *Complexity in implementation* | *4 to 12 months* | *Very high cost* | *Highly Required* | *No formal certification required* | *Moderate* |
| HITRUST CSF | *Comprehensive framework for managing data security, integrating multiple regulatory requirements (HIPAA, NIST, PCI DSS) into a single security framework.* | *Primarily for health sector* | *Security, privacy, and regulatory compliance, integrating multiple standards (HIPAA, NIST, PCI DSS).* | *Yes* | *Complex and resource-intensive* | *8 to 18 months* | *Extremely high cost* | *Required* | *Certification required* | *Moderate* |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PCI DSS | *Security controls and requirements to protect payment card data, ensuring that organizations securely process, store, and transmit credit card information.* | *Payment credit industry* | *Payment card data protection and security controls for safeguarding payment systems.* | *Yes* | *Limited scope beyond cardholder data protection* | *6 to 12 months* | *Very high cost* | *Highly Required* | *Certification required* | *Moderate* |
| CIS RAM | *Risk assessment method that aligns with CIS Controls, allowing organizations to assess their maturity and implement security controls effectively.* | *Applicable to all industries* | *Cybersecurity maturity assessment based on the implementation of CIS Controls.* | *Yes* | *Requires stringent controls and limited in scope* | *3 to 6 months* | *High cost* | *Required* | *No formal certification required* | *Moderate* |
| FSSCC CAT | *Assesses the cybersecurity posture of financial services institutions, aligning with the NIST CSF and providing a maturity-based evaluation tool.* | *Financial services institutions* | *Cybersecurity risk management, maturity assessment, and compliance for the financial sector.* | *Yes* | *Limited public information, may lack detail* | *4 to 8 months* | *High cost* | *Required* | *No formal certification required* | ***Low*** |
| CERT-RMM | *Measures an organization's maturity by focusing on processes like RM, IRP, and service continuity.* | *Applicable to all industries* | *Organizational resilience, risk management, incident response, and service continuity.* | *Yes* | *Complex, resource-intensive implementation* | *6 to 12 months* | *High cost* | *Required* | *No formal certification required* | *Moderate* |
| SSE-CMM | *Focuses on assessing and improving security engineering processes within organizations, particularly those related to systems development and security integration.* | *Applicable to all industries* | *Security systems engineering and process maturity, particularly for secure systems development.* | *Yes* | *Limited to security engineering process* | *6 to 12 months* | *High cost* | *Highly Required* | *No formal certification required* | *High* |
| ITIL | *Provides a framework for IT service management (ITSM), focusing on aligning IT services with business needs* | *Applicable to all industries* | *IT service delivery, operations, and aligning IT services with business needs.* | *No* | *Complex to implement* | *6 to 12 months* | *High cost* | *Highly Required* | *Certification required* | *High)* |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| NICE CSF | *Structured framework for improving and developing cybersecurity workforce skills and categorizing cybersecurity roles to meet industry needs.* | *Applicable to all industries* | *Cybersecurity workforce development, skills identification, and role categorization.* | *Yes* | *Limited guidance on technical controls* | *4 to 8 months* | *Medium cost* | *Required* | *No formal certification required* | *Moderate* |
| CREST | Sets standards for cybersecurity testing and provides accreditation for organizations and professionals performing penetration testing, incident response, and other security services. | *Applicable to all industries* | Cybersecurity testing standards, accreditation for penetration testing, and incident response. | Yes | Skills and workforce-based implementation | 6 to 12 months | Very high cost | Highly Required | Certification required | Moderate |
| CCSMM | Comprehensive cybersecurity maturity model to assess and improve the cybersecurity capabilities of organizations, particularly in critical infrastructure. | *Applicable to all industries* | Cybersecurity maturity assessment and capability improvement for critical infrastructure and large organizations. | Yes | Requires adherence to specific certification standards. | 6 to 12 months | High cost | Required | No formal certification required | Moderate |

*Table 1 - Comparative Analysis on Existing Frameworks*

## 2.2. Related works

### *Works Related to Ethiopian Context*

Numerous researchers have examined the state of information security management and cybersecurity readiness in Ethiopia, with a particular focus on the financial, healthcare, and educational sectors. Many studies have evaluated security maturity levels and the implementation of global security frameworks like ISO 27001 and NIST SP 800 across various industries. [12] performed a case study evaluating information security management at Ethio Telecom using the ISO 27001:2013 framework. The research highlighted the necessity for enhanced security practices and offered recommendations based on the ISO framework. However, the study was limited by its concentration on a specific version of ISO 27001, excluding the potential applicability of newer or alternative frameworks that could be utilized across different industries. Similarly, [39] developed an information security framework specifically for the Ethiopian banking sector, proposing a model that integrated ISO 27001 and NIST SP 800 standards. While this framework comprehensively addressed these international standards, it lacked a wider perspective that might incorporate other frameworks relevant to emerging threats in banking. [73] adopted a distinctive approach by creating a framework centered on information security awareness delivery methods. Although the researcher suggested a role-based training approach, emphasizing customized awareness programs based on employee roles, the study's scope was restricted to awareness programs, overlooking the broader context of security maturity assessment, which is crucial for a comprehensive view of organizational security. In addition to that, [40] investigated the practices, challenges, and prospects of information security policies within Ethiopian banks. While the study recognized the importance of security culture and emphasized the need for employee training, it primarily concentrated on human and procedural aspects, neglecting the maturity dimension crucial for assessing an organization's information security preparedness.

To look another works, [74] sought to evaluate mobile banking security protocols, recommending the implementation of appropriate safeguards to enhance the banking sector's defense against mobile threats. However, the research was constrained by its narrow scope, focusing mainly on mobile banking security and overlooking broader digital banking vulnerabilities. Moreover, focusing on cybercrime governance, [2] examined cybercrime prevention and management in Ethiopia through document analysis and review, focusing on cybercrime governance. The study

highlighted the lack of a robust legal framework and governance structure for cybersecurity. Nevertheless, it heavily emphasized governance aspects while neglecting technological and operational considerations that could complement the governance framework. Research efforts have been made to evaluate security maturity across various sectors. [75] examined information security management maturity in Addis Ababa hospitals, revealing low security maturity and weak policy implementation based on the ISO 27002 framework. However, this study was limited to hospitals, excluding other crucial sectors such as finance and education. Similarly, [76] identified similar low security maturity levels in Ethiopian public universities but did not offer a comprehensive framework to address these issues. Exploring the banking perspective, [38] assessed information system security maturity in Ethiopian banks, uncovering inconsistent security implementations and governance structures, yet also failed to propose a comprehensive solution. Where [77] investigated cyber hygiene practices among Ethiopian commercial bank employees, noting poor security habits, particularly in password management and phishing awareness, but did not extend the study to evaluate the banks' overall security infrastructure maturity. Additionally, human factors in information security were explored by [19], who proposed a framework focusing on the influence of human factors on information systems security in Ethiopian commercial banks. However, this study was limited by its narrow focus on human factors, neglecting technical and organizational aspects. To mention other Ethiopian scholars, in a broader assessment of cybersecurity preparedness, [78] examined the readiness of Ethiopian banks, [75] emphasized the need for regular cybersecurity awareness programs, [79] conducted a gap analysis on incident response management and [80] analyzed the role of regulatory frameworks in digital financial services and Ethiopian banks. However, their focus remined on preparedness, training and awareness, incident response and regulatory challenges without delving into the broader maturity framework and long-term resilience strategies.

| Authors | Purpose of the Study | Research Methodology | Key Findings | Limitations |
|---|---|---|---|---|
| [12] | Assess information security management at Ethio Telecom using the ISO 27001:2013 framework. | Case study | Suggested improvements based on ISO 27001. | Focuses on a specific ISO27001:2013 framework |
| [74] | Evaluate the implementation of mobile banking security protocols in Ethiopia | Mixed approach | Suggested proper mobile money security protocol | Limited coverage on mobile banking security |
| [39] | Propose an information security framework for the banking industry in Ethiopia. | Case study | Suggested a framework based on ISO 27001 and NIST SP 800. | Proposed Framework on ISO and NIST only |
| [73] | Design a framework for selecting effective information security awareness delivery methods. | Case study | Proposed role-based training method | Focus only on awareness; doesn't cover maturity |
| [40] | Study the practices, challenges, and prospects of information security policy in the Ethiopian banking industry. | Qualitative approach. | Identified security culture and training | Focuses mainly on people and process; doesn't include maturity |
| [2]) | Assess the state of cybercrime governance in Ethiopia. | Document analysis and review | Lack of legal framework and & structure for cybersecurity | Focus on cybercrime governance |
| [75] | Assess the maturity level of information security management at hospitals in Addis Ababa using ISO 27002. | Case study | Low-security maturity and policy enforcement in Hospitals | Tailored to hospitals; doesn't recommend framework |
| [76] | Assess the information security maturity level of Ethiopian public universities. | Survey-based research | Identified that public universities have a low-security maturity level | Tailored to public universities; doesn't recommend a framework |
| [77] | Assess cyber hygiene practices among employees of Ethiopian commercial banks. | Survey-based research | Poor security hygiene among employees | Doesn't reflect on cyber maturity |
| [38] | Investigate the current information system security maturity level in the banking industry in Ethiopia. | Qualitative approach | Identified inconsistent security implementations and proper structure | Focuses on investigations; doesn't propose a framework |
| [19] | Develop a framework for the influence of human factors on information systems security in commercial banks in Ethiopia. | Case study | Proposed a framework to influence human factors | The proposed framework is too narrow on human factors |
| [78] | Examine the cybersecurity preparedness of Ethiopian banks | Mixed approach | Revealed inadequate cybersecurity preparedness | Focused on CS preparedness in banks |
| [36] | Assess the impact of insider threat in Ethiopian banks | Survey-based study | Recommended regular training programs | Focuses mainly on CS awareness |
| [79]) | Conduct a gap analysis of information security incident response management in an Ethiopian bank. | Case study | Identify gaps in the incident response standardized framework | Focuses on incident response management |
| [80] | Analyze the role of regulatory frameworks in digital financial services | Qualitative approach | Current regulatory frameworks are insufficient to address the cybersecurity challenges of DFS | Focused on regulatory issues only |

*Table 2 - Related Works to Ethiopian Context*

*International Context*

Several international scholars have contributed to the field of cybersecurity maturity assessment, with a focus on various industries including education, finance, critical infrastructure, and healthcare. These studies have primarily sought to develop and assess the maturity of cybersecurity frameworks and their effectiveness in addressing sector-specific challenges.

Researchers [17] and [18] developed comprehensive cybersecurity maturity assessment frameworks specifically for higher education institutions in the UK and Saudi Arabia. These frameworks included maturity models designed to address the unique cybersecurity challenges faced by this sector. However, the studies were confined to higher education, leaving their applicability to other industries, particularly the banking sector with its distinct cybersecurity threats, unexplored. Similarly, [54] created an information security maturity model based on the NIST Cybersecurity Framework (NIST CSF), while [65] proposed a cybersecurity capability maturity model grounded in C2M2. Additionally, [62] concentrated on standardizing cybersecurity roles and competencies across industries using the NICE framework to assist organizations in determining their cybersecurity maturity. These studies, however, demonstrated limitations by focusing on specific sectors such as critical infrastructures and narrowly emphasizing NIST CSF, C2M2, and NICE framework. They failed to consider the unique cybersecurity requirements of the banking industry, which demands specific skill sets and overlooked other internationally recognized frameworks that could offer broader applicability. Although [81] developed CAT5, an instrument for assessing IT governance maturity using the COBIT 5 framework, their study primarily concentrates on IT governance, overlooking crucial cybersecurity elements necessary for comprehensive security management. Similarly, [58] and [63] introduced the CERT Resilience Management Model (CERT-RMM), a maturity model centered on operational resilience, and a maturity model specifically for incident response management, respectively. However, these models' strong emphasis on incident response and resilience fails to address the need for broader cybersecurity aspects. Additional international researchers have explored cybersecurity maturity-related topics, including [82] cybersecurity framework for cybersecurity audit, [83] a dynamic capability maturity model for continuous improvement in cybersecurity, [84] C2M2 model for critical infrastructure, [85] M2HCS framework tailored to assess cybersecurity maturity in healthcare cloud services, [86] Cybersecurity Resilience Maturity Measurement (CRMM) framework to help organizations in Africa measure their cybersecurity resilience, [11]

cybersecurity maturity model and a self-assessment toolkit to measure cybersecurity maturity levels in academic institutions, [21] systematic literature review of information and cybersecurity maturity models, and [23] governance of information security in banking systems. Despite addressing these issues individually, their research has limitations in terms of implementation strategy guidance, inadequate coverage of cybersecurity maturity components, limited applicability, and lack of a new proposed framework.

| Authors | Purpose of the Study | Research Methodology | Key Findings | Limitation |
|---|---|---|---|---|
| [17] | Propose a holistic cybersecurity maturity assessment framework for higher education institutions in the UK | Case study | Developed a maturity model tailored for higher education | Limited to the higher education sector |
| [54]) | Propose an information security maturity model based on the NIST Cybersecurity Framework | Mixed approach | Proposed a maturity model to assess NIST CSF implementations, | Focused on NIST CSF |
| [50] | Propose CAT5, a tool for measuring IT governance maturity using the COBIT 5 framework | quantitative analysis | Ensure the effectiveness of the CAT5 tool to measure COBIT 5 maturity | Heavily focuses on IT governance and COBIT 5; doesn't address cybersecurity components |
| [65] | Develop a cybersecurity capability maturity model (C2M2) for critical infrastructure | Qualitative approach | Suggests C2M2 for critical infrastructure sectors to assess cybersecurity capability | Limited to the critical infrastructure sector |
| [62] | Provide a cybersecurity workforce framework to standardize roles and competencies in the field | Expert interviews | Suggested NICE Framework to standardize cybersecurity roles and competencies for organizations | Doesn't address specific cybersecurity needs for the banking sector |
| [58] | Propose a maturity indicator level scale for measuring cybersecurity capabilities | Qualitative approach | Suggested CERT-RMM maturity model to assess organization's cybersecurity maturity | Heavily focuses on operational resilience |
| [63] | Develop a maturity model for establishing incident response management capabilities | Case study | Developed a maturity model tailored for incident response capabilities | Limited to incident response management |
| [82] | Develop a comprehensive cybersecurity audit model to enhance cybersecurity assurance | Case study | Proposed a Cybersecurity Audit Model (CSAM) to improve cybersecurity assurance | Limited to cybersecurity audit |
| [83] | Propose a dynamic capability maturity model for improving cybersecurity | Case study | Proposed a framework for continuous improvement in cybersecurity capabilities | Too generic |
| [84] | Examine cybersecurity capability maturity models for providers of critical infrastructure | Qualitative approach | Recommended C2M2 implementation for critical infrastructures | Focuses on C2M2; lack of detailed implementation |
| [85] | Develop a cybersecurity maturity model for healthcare cloud security (M2HCS) | Case study | Proposed a framework for healthcare organizations using cloud services | Limited to the healthcare sector |
| [86] | Develop a cybersecurity resilience maturity measurement (CRMM) framework | Case study | Propose a framework that helps organizations in Africa measure and improve their cybersecurity resilience | Limited to cybersecurity resiliency |
| [18] | Propose a cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia | Case study | Proposed a framework for higher education that focuses on risk management and incident response | Limited to the education sector. |
| [11] | Propose a cybersecurity maturity model and self-assessment toolkit | Case study | Proposed a self-assessment toolkit to measure cybersecurity maturity levels | Limited to academic institutions; too narrow industry application |
| [21] | Conduct a systematic literature review of information and cybersecurity maturity models | Systematic literature review | Identified strengths and limitations of cybersecurity maturity models | No proposed framework |
| [23] | Develop a framework for the governance of information security in banking systems | Case study and qualitative analysis | Proposed a framework for the banking sector to align business needs with cybersecurity objectives | Limited to cyber governance; doesn't address maturity |

*Table 3 - Related Works in International Context*

# Chapter Three

## 2. Research Methodology

This chapter presents the research design and methodology of the study. The researcher goes into further detail about the research method, research approach, data collection techniques, sample and study setting selection, research process, kind of data analysis, validation, and reliability in this section. This chapter provides a thorough explanation of the tools utilized to collect data as well as the steps taken to carry out this analysis. The elements of this study are described, starting with the population as a whole and ending with the sampling strategies applied to the questionnaire. Finally, this chapter concludes with a thorough description of the chosen mode of analysis, data validation methods and reliability techniques.

### 3.1 Research Design

[87] defines research design as a systematic technique for collecting, analyzing, and interpreting data from a single study. It demonstrates the researcher's logical and coherent integration of numerous study aspects. This design ensures that the study problem is properly addressed by developing techniques for data collection, measurement, and analysis. The basic goal of a research design is to guarantee that the facts and information collected allow for a coherent and unambiguous approach to the research problem.

The research design acts as the study's framework, connecting all of the research components. [88] defines it as a rigorous design of analytical procedures and data acquisition techniques. [89] outlines three possible study design types: descriptive, explanatory, and exploratory. This classification was created to apply to a variety of study fields. Among these research methodologies, this study uses a descriptive research design. Descriptive research seeks to provide an accurate and systematic description of a population, situation, or phenomena, answering the what, where, when, and how questions [90]. Unlike other research design procedures, descriptive research enables researchers to observe and investigate variables using a variety of ways without controlling or manipulating them. This method is more suited for studies that seek to discover features, frequency, trends, and classifications.

#### 3.1.1 Research Approach

There are three basic techniques to conducting research: quantitative, qualitative, and mixed methodologies, and we anticipate the sort of data needed to answer the study question. This study

uses a qualitative approach to attain its objectives and collect the necessary data. Qualitative research is a methodological technique that seeks to comprehend and analyze human experiences, behaviors, and social phenomena in their natural contexts. It stresses the collection and analysis of non-numerical data, such as words, images, and observations, to achieve profound insights into complicated societal situations [91]. This technique is especially useful in domains such as psychology, education, and social sciences, where researchers can investigate the intricacies of human experiences and perspectives.

In this study, the qualitative approach was utilized to investigate attitudes, obtain in-depth opinions and experiences of respondents on the topic matter, and collect data required to respond to the research question.

### 3.1.2 Study Setting

This research is conducted on selected nine bank headquarters sites located in Addis Ababa from a total of 31 banks according to (the NBE website) the respondents will be directors and IT/CS department professionals, who are responsible for cyber security issues.

### 3.1.3 Sample Selection

The sample is a part of objects taken from a population, which is representative of the population. For this study, the researcher employed stratified probability sampling to select 9 banks among the available 31 banks according to the data retrieved from the National Bank of Ethiopia website. Those banks are grouped into two groups (strata) based on their existence. Governmental and Private and the researcher picked 3 governmental banks and 6 private banks.

### 3.1.4 Study Participants

A research participant is someone who participates in research and will answer the questions posed by this study. The study sample participants in this study were chosen based on their special connection to the topic under study, as well as sufficient and relevant professional skills in the field of cybersecurity. The sample objects are chosen based on their expertise and position within the study area. The study's target population is the overall IT/CS department leaders and professionals at each sampled governmental and private bank's HQs.

## 3.2 Research Technique

In this study, we conducted exploratory research through thematic analysis to examine the cybersecurity maturity level of governmental and private Ethiopian banks. The research technique

is an important aspect of a study since it helps to determine how to achieve the research's general and specific objectives, the data collection instrument, data analysis, and presentation. Which collectively strives to solve the research questions.

### 3.2.1 Data Collection

A qualitative research approach was utilized to collect data through interview questions and document analysis. The primary data was collected through interview questions. The secondary data was collected through document analysis as it was gathered through document analysis (in house developed frameworks) and a review of the literature to better understand the actual cybersecurity maturity level of the Ethiopian governmental and private banking sector.

### 3.2.2 Interview

An interview is a method in which the interviewer asks questions to elicit information from the respondent [92]. A semi-structured interview framework was created and used in this study to obtain qualitative data. The interview helps to collect attitudes and experiences from the target communities. We carefully picked the interviews to ensure that the correct answer was obtained. Thus, the target respondents were IT/CS directors, managers, and professionals from various banks. It was performed face to face and through phone in cases where respondents were unavailable owing to various reasons.

### 3.2.3 Document Analysis

Document analysis mainly helps the researcher in determining the validity and reliability of interview questions responses. So, we have deployed a document analysis to strengthen the study by referring to various documents, such as journal articles, in-house developed frameworks, conference papers, and cybersecurity-related documents i.e., cybersecurity policy, cybersecurity risk management framework, cybersecurity maturity assessment frameworks, and other bank-related materials. The document analysis is utilized as a secondary data source to supplement and complement the data obtained from the other instruments.

In this study, qualitative data analysis entails detecting common patterns among replies and critically analyzing them to fulfill study goals and objectives. The qualitative data is examined by open coding. It is provided in a form that provides explanations, understanding, and interpretation of the phenomena in the following chapter of the study.

## 3.3 Ethical Consideration

Ethical considerations play a crucial role in developing and implementing a Cybersecurity Maturity Assessment Framework (CMAF) for banks. The framework should not only focus on technical aspects but also incorporate ethical principles to ensure responsible and trustworthy cybersecurity practices. Interestingly, while numerous studies have looked into ethical and privacy concerns in cybersecurity research, there are no standardized techniques for ensuring proper ethics and privacy standards [93]. This gap emphasizes the need for a comprehensive ethical framework adapted specifically to cybersecurity research and assessment in the banking industry. Such a paradigm could aid researchers and practitioners in conducting ethical cybersecurity assessments and research.

One of the most important ethical considerations is protecting consumer data privacy and confidentiality. Banks manage sensitive financial data, therefore any evaluation framework must prioritize protecting it from illegal access or breaches [94]. We followed the below ethical issues when conducting his research:

- The anonymity of the institution was preserved throughout the entire research,
- The interview was conducted based on the respondent's consent,
- The researcher focused mainly on manipulating data from both primary and secondary resources only,
- We tried to utilize the original responses of participants while analyzing the results,
- All the manuscripts, documents, standards, and other resources that have been used in this research are properly acknowledged and cited.

Lastly, ethical considerations are incorporated as an important role throughout the procedure. This involves evaluating the bank's adherence to ethical norms in data processing, decision-making procedures, and overall cybersecurity measures [94].

## 3.4 Chapter Summary

The chapter presented the study's research design and methodological content. The design and methodology strategies are briefly outlined in terms of how they might be used to better answer research questions and achieve the study's objectives. This study employs a qualitative research approach to collect data from participants, outlines the research strategy, describes the study environment in-depth, reveals the sampling strategies employed, and identifies the study population. Also included are research strategies and methodologies that allow the researcher to

present data-gathering tools, procedures, sources, and presentations. Finally, the analysis and data presentation method of the study has been discussed. The researcher analyzed open coding for qualitative data.

# Chapter Four

## 3. Proposed Solution

This proposed framework is designed to assess and enhance the cybersecurity maturity of the banking sector. It integrates international best practices from established regulations like GDPR while addressing the unique challenges faced by Ethiopian banks. The framework comprises key domains such as cyber governance, risk management, business continuity and disaster recovery, awareness and culture development, personal data protection, mobile money security, supply chain security, ATM security, IRP, network security and information sharing and collaboration, offering a customized approach to improve the security posture of Ethiopian banks. By aligning cybersecurity initiatives with local regulations and global standards, this framework enables banks to systematically identify, prioritize, and mitigate cybersecurity risks, ensuring a resilient and secure operational environment.

### 4.1 Overview of the Proposed Framework

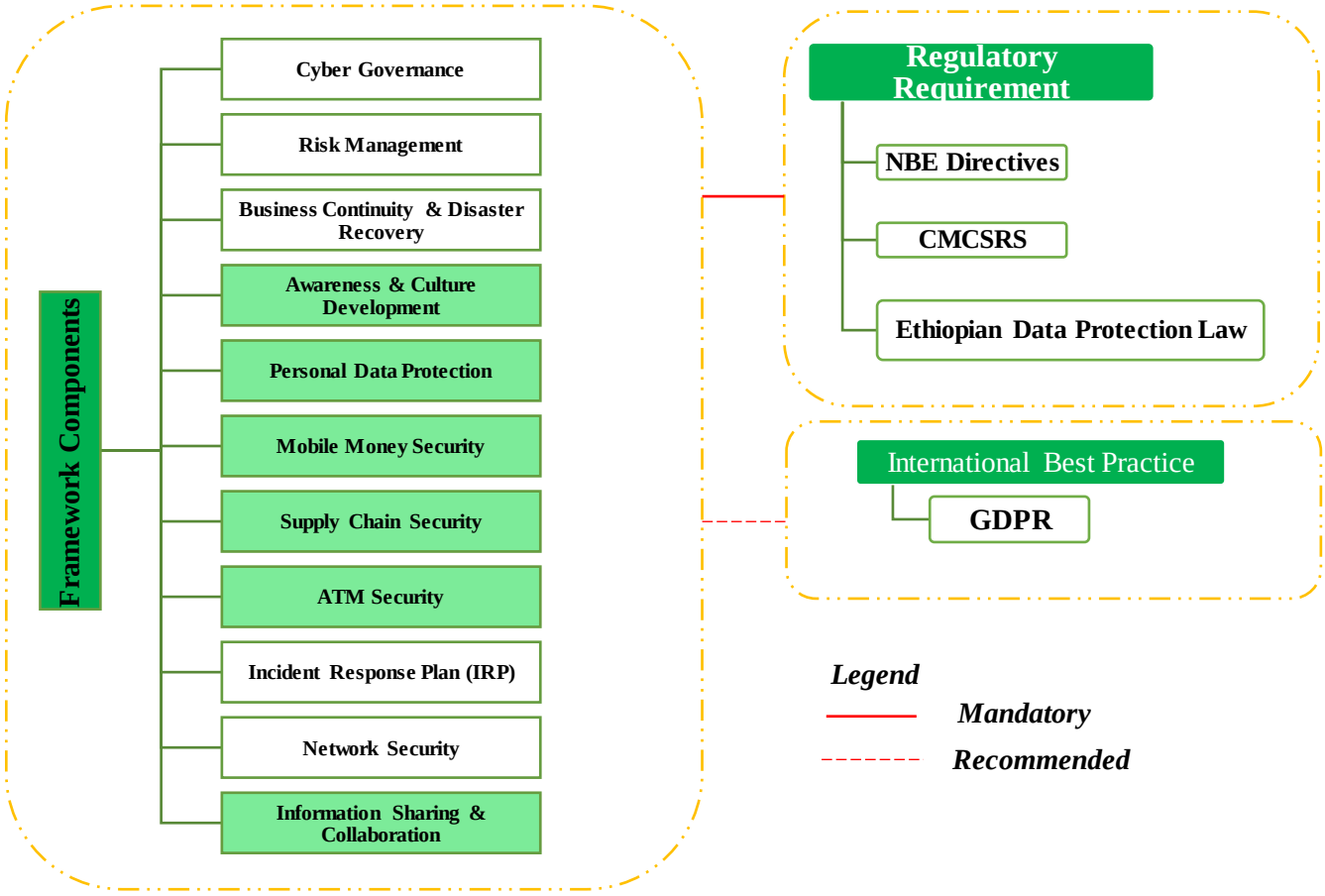


*Figure 3 - Proposed Cybersecurity Maturity Assessment Framework*

## 4.2 Component Description

In this section, all the components of the proposed cybersecurity maturity assessment framework are explained in detail. These descriptions underline how each component refers to the specific needs and challenges within the banking sector while incorporating international best practices. Moreover, a table shown in Annex B demonstrates the mapping of domain, sub-domain, controls, and mapped reference standards.

### Cyber Governance

Cyber Governance involves the establishment of a structured framework for strategically managing cybersecurity within a bank. This framework includes the implementation of a cybersecurity strategic plan, the development of policies and procedures, and the creation of processes that support the guiding framework. It also involves defining roles and responsibilities and establishing a formal cybersecurity structure, governed at the highest levels of the organization. Given the dynamic and disruptive nature of cyberspace, particularly within the banking threat landscape, cybersecurity should be structured as a standalone entity within the organization [52]. This separation allows for more focused management and resource allocation, ensuring that cybersecurity is treated as a priority.

To foster an effective cybersecurity culture, the structure must ensure that the cybersecurity department is both authoritative and resourceful. This empowers the department to implement necessary controls and respond to emerging threats promptly. Additionally, strong cyber governance is critical for ensuring accountability and aligning cybersecurity initiatives with the bank's overall strategic goals [54]. As cybersecurity risks evolve, continuous adaptation is necessary to ensure that governance structures remain resilient and proactive in addressing potential threats [59].

### Risk Management

This risk management component involves risk assessment, risk treatment, risk evaluation, and reporting cybersecurity risks that the banks are facing [54] [52]. By utilizing robust risk management methods, banks can proactively address vulnerabilities and reduce the likelihood and impact of cyber threats. As mentioned above, the proposed framework suggests four risk management phases [59]. Risk assessment process entails proactively identify, assess, and mitigate cybersecurity risks to protect organizational assets from damage. [66] Risk treatment refers to the development and implementation of risk treatment strategies to address identified cybersecurity

risks effectively. [67] The risk evaluation and reporting phase focuses on evaluating the effectiveness of cybersecurity controls to adapt to evolving threats and to establish a healthy reporting mechanism to communicate cybersecurity risk status and remediation efforts.

### Business Continuity & Disaster Recovery (BC & DR)

BC & DR planning ensures that banks can maintain critical operations during and after a cybersecurity incident. [59] [54] At the time of system breakdown, which is rarely a common experience in the banking sector, an outstanding set of plans should be in place to let the business continue its operation without interruption. [95] Whereas disaster recovery focuses on developing strategies and processes to quickly recover from known disruptions, minimize downtime, and maintain customer trust [52]. It includes infrastructure resilience to maintain failover mechanisms, backup systems, data recovery procedures, regular testing of recovery plans, and continuous improvement.

### Awareness and Culture Development

Specialized cybersecurity training programs are crucial for meeting the unique requirements of professionals in sectors such as finance, healthcare, and critical infrastructure. Studies indicate that personalized learning approaches are more successful in cultivating relevant technical and managerial abilities [62]. Guidelines like the [54] stress the importance of job-specific training that corresponds to organizational objectives. Enhancing technical cybersecurity proficiency through practical sessions, interactive laboratories, and industry events enables professionals to remain current with the latest security innovations and trends. Research demonstrates that ongoing professional growth through these activities cultivates deeper expertise and improves the overall cybersecurity stance of organizations [96]. Standards such as CREST advocate for focused workshops in areas including penetration testing and incident response [63].

Implementing a methodical cybersecurity awareness development strategy is vital for educating non-technical personnel about security best practices. Awareness initiatives based on standards like ISO 27001 underscore the necessity of training all employees to identify potential threats, such as phishing attempts or insider risks [52]. Studies show that consistent awareness training decreases the probability of human error in cybersecurity incidents [97]. Consistent cybersecurity awareness programs should be implemented to keep employees informed about emerging threats and company policies. As per NIST SP-800-50, continuous awareness training strengthens the

security culture within organizations and encourages proactive behavior in recognizing and addressing security risks [56]. Establishing a professional career trajectory for IT and cybersecurity experts helps align individual growth with organizational needs. Frameworks such as NICE CSF offer structured career paths, linking skills development to cybersecurity roles and competencies. Research emphasizes the significance of aligning career progression with formal education, certifications, and on-the-job training to build a robust cybersecurity workforce [62].

Professional certifications such as CISM and CISSP play a crucial role in confirming the competence of information technology and cybersecurity experts. These internationally recognized credentials demonstrate that individuals have the required expertise to safeguard vital resources and networks [98]. Studies show that professionals with certifications are more capable of implementing sophisticated cybersecurity measures and overseeing intricate systems [99]. Establishing a thorough strategy for retaining cybersecurity talent is vital in tackling the shortage of skilled professionals in this field. Research suggests that high employee turnover in cybersecurity is attributed to factors like job-related stress, unclear career advancement paths, and insufficient rewards [100]. CREST highlights the necessity of offering competitive pay, opportunities for professional growth, and a favorable work atmosphere to keep top-tier talent [63].

### Personal Data Protection

This component focuses on safeguarding the personal and financial data of customers in compliance with data protection regulations such as [101] Personal Data Protection Proclamation No 1321/2024. This process includes implementing data encryption, access controls, and regular audits to ensure that personal data is clearly collected, stored, processed, analyzed, transmitted securely, protecting against data breaches and unauthorized access. Moreover, adding this component to the whole framework would give the banks an advantage of gaining trust from their customers. To fully address this component into ground, the following core controls are included:

- Data classification and encryption,
- Anonymization and data masking,
- Pseudonymization,
- Data Protection Impact Assessment,
- Data Loss prevention,

- Data retention and disposal

### Mobile Money Security

With mobile banking becoming more popular in Ethiopia, financial institutions must prioritize the security of mobile money transactions. This component addresses specific risks associated with mobile platforms, such as SIM swap fraud and unauthorized access, to ensure that users can rely on mobile banking services for financial transactions. [74] fraudsters are increasingly targeting mobile money platforms in Ethiopia, necessitating the implementation of effective security procedures in order to maintain customer trust. To secure these platforms, multi-factor biometric authentication for transactions is required, as well as secure mobile money development processes that adhere to secure coding principles. Furthermore, improving fraud detection algorithms and monitoring suspicious activity on financial transactions are critical steps toward preventing illegal access and financial loss [102]. These measures help to mitigate emerging threats and ensure that mobile money transactions are secure. As part of a larger cybersecurity maturity assessment methodology, mobile money security is critical for the banking sector to handle the cybersecurity threats provided by mobile transactions [52].

### Supply Chain Security

Supply chain security takes on the threats posed by third-party suppliers, vendors, and business partners. The growing reliance on external partners creates additional risks, especially if these firms do not conform to the bank's high cybersecurity standards. According to [103] a lack of security among third-party providers can provide access vectors for assaults on crucial banking infrastructure. As a result, this component ensures that all external partners adhere to the bank's cybersecurity requirements and contractual responsibilities, lowering the risk of breaches coming from less secure areas of the supply chain.

This component's key parts include doing due diligence throughout the vendor selection process, writing contractual agreements outlining security standards, and implementing continuous monitoring methods. Furthermore, vendor evaluations and audits are essential for maintaining security throughout the supply chain, ensuring that third-party partners do not introduce vulnerabilities into the bank’s operations [54].

### ATM Security

Despite the increasing popularity of mobile and online banking platforms, ATMs still provide crucial services, especially in areas where cash-based transactions are prevalent [12]. As a result, protecting ATMs from various threats is essential not only for preserving customer confidence but also for ensuring the operational stability of financial institutions. Given the financial and reputational risks associated with ATM breaches, it is imperative for the banking industry to implement the proposed cybersecurity maturity assessment framework.

Furthermore, ATMs function as decentralized systems often linked to banking networks, creating potential vulnerabilities for cybercriminals to exploit. Attackers may take advantage of unpatched ATM software or weaknesses in ATM communication channels to infiltrate the larger bank network, jeopardizing sensitive financial information [67]. Thus, securing ATMs also enhances the overall cybersecurity stance of the institution, preventing attackers from using ATMs as gateways for more extensive attacks. By implementing specific controls for physical security, network protection, transaction monitoring, and incident response, banks can mitigate risks associated with ATM operations, reducing fraud, theft, and operational disruptions.

Finally, regulatory bodies, including the [67] and [54], require security controls for ATMs as part of broader mandates for safeguarding financial systems. Implementing a comprehensive ATM security framework ensures adherence to industry regulations and standards while demonstrating a commitment to protecting customer assets and maintaining the integrity of banking operations.

### Incident Response Plan (IRP)

An incident response plan outlines an organized approach for recognizing, responding to, mitigating, and recovering from cybersecurity issues. According to [59], having set protocols for identifying and controlling events is critical for mitigating the impact of security breaches and guaranteeing a timely return to regular operations. This component includes processes like incident detection, containment, eradication, recovery, and post-event analysis to assess lessons gained and improve future security postures.

The integration of Security Incident and Event Management (SIEM) solutions into an incident response architecture can dramatically improve a bank's ability to detect attacks in real time. A well-developed incident response plan lessens the effect of cyber-attacks and allows the bank to conduct post-incident reviews to identify gaps in its response strategy and improve future resilience [54]. Banks can achieve this component's objectives by integrating these tools, along

with dynamic response plans and data recovery strategies, into their cybersecurity maturity assessment frameworks.

### Network Security

Network security is a critical component in safeguarding a bank's infrastructure against cyber threats. Firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), secure network architecture, patch management, and encryption are among the procedures used to protect the bank's network. Because banks handle sensitive financial information, securing their network infrastructure is crucial to safeguarding the integrity of banking operations [95].

Firewalls and IDS/IPS are network security technologies that monitor network traffic and prevent unwanted system access. Encryption protects data in transit from interception, while patch management addresses system vulnerabilities by providing security upgrades on a timely basis [54]. These measures are critical for protecting against network-based assaults and preserving confidentiality, integrity, and availability of critical banking systems. Additionally, cloud security component offers flexibility, scalability, and cost-efficiency, but they also introduce unique security challenges that traditional security frameworks may not fully address. So, the banking sector can adopt cloud solutions securely and confidently while maintaining compliance with regulatory requirements and protecting customer data. [67].

### Information Sharing & Collaboration

This ideal component enables banks to participate in information-sharing initiatives with bank to bank, other financial institutions, regulatory bodies, and cybersecurity organizations. Automated Platforms enable banks to share cyber threat information in real-time, reducing the window of vulnerability [104]. This component emphasizes the importance of creating a collaborative environment where entities share cybersecurity related information via secure communication channels [105]. Additionally, the framework supports the engagement with intelligence communities and law enforcement agencies to enhance banking industry ability to detect and respond to cyber threats. [106] cross-functional collaboration between banks and intelligence agencies fosters real-time threat detection and strengthens cyber resilience. Moreover, inter-banking collaborations and joint drills, which will be implemented through Information Sharing Centers, should be available in a formal agreement as they set out clear scope and conditions for sharing data and conducting the exercise.

### Regulatory Compliance

This component ensures that banks align their cybersecurity practices with both local regulatory requirements and international laws as a best practice. In our context, this includes compliance with mandatory regulatory requirements like [107] the Critical Mass Cyber Security Requirement Standard (CMCSRS), [101] Personal Data Protection Proclamation No. 1321/2024, and Computer Crime Proclamation [108]. By complying with these regulations, the banking sector can mitigate regulatory risks and ensure their cybersecurity strategies. Moreover, [109] NBE Directive No. SBB|83|2022 has introduced a critical component that are related with cyber maturity aspects. To mention, some of them, Article 7 sub article 7.2 require banks to address physical access and network securities, BC & DR, IRP, IT Vendor and Third-party Management, Data Privacy and Security components.

### International Best Practices

This component integrates well recognized global standards, such as the General Data Protection Regulation (GDPR) [110], into the proposed cybersecurity maturity assessment framework. By incorporating GDPR principles, banks may ensure that important areas of data privacy and security are addressed. The framework is an EU rule, but its impact is global. For most companies must comply with [111], making it a significant norm for cybersecurity assessments around the world. It also encourages banks to take a risk-based approach to data protection, in line with current cybersecurity procedures. This technique aids in prioritizing security solutions based on the probable consequences of data breaches. It also emphasizes organizational accountability by mandating clear policies, procedures, and documentation. This is consistent with cybersecurity maturity models, which analyze an organization's governance structures and processes. Additionally, it promotes the concept of privacy by design, encouraging organizations to consider data protection from the outset of any project or system development. This proactive approach enhances overall cybersecurity posture. [112] It mandates strict breach notification requirements, which can be integrated into cybersecurity incident response plans, improving an organization's ability to detect, respond to, and report security incidents. By incorporating GDPR's provisions for data subject rights (e.g., right to access, right to be forgotten), banks can demonstrate a higher level of maturity in managing and protecting personal data. GDPR's requirements for managing data processors align with cybersecurity best practices for vendor risk management, enhancing supply chain security. [113] The rules on international data transfers can be incorporated into

cybersecurity frameworks to ensure secure and compliant cross-border data flows. Additionally, it encourages regular reviews and updates of data protection measures, aligning with the concept of continuous improvement in cybersecurity maturity models. By incorporating GDPR as a best practice in a Cybersecurity Maturity Assessment Framework (CMAF), banks can demonstrate a commitment to data protection, enhance their overall security posture, and align with internationally recognized standards.

These components collectively form a comprehensive framework that is both tailored to the specific needs of the Ethiopian banking sector and aligned with international best practices. By implementing this framework, banks can significantly enhance their cybersecurity maturity, better protect their assets, and ensure regulatory compliance.

### 4.3 Framework Measurements

Concerning each cybersecurity maturity assessment framework components outlined above, the framework defines a five-level of maturity that serves as the basis for understanding banking sector cybersecurity maturity and provides a foundation for capability improvement planning.

| MATURITY LEVEL | DESCRIPTION |
|---|---|
| *Ad hoc - 0* | *Cybersecurity practices are intermittent, reactive, and disorganized. There are no structured processes, and cybersecurity measures, no established procedures for managing cybersecurity risks, and protective measures are implemented only when specific threats arise or after an incident has occurred. This lack of structured processes leaves the institution vulnerable to evolving cyber threats, as there is no proactive or systematic approach to safeguarding sensitive financial data or customer assets.* |
| *Initial - 1* | *At this level, the bank may have begun to build some basic cybersecurity procedures, but they are uneven and not fully integrated into entire business operations. There may be sporadic efforts to fix cybersecurity issue such as patching vulnerabilities and responding to incidents.* |
| *Defined -2* | *There is a formal way to address cybersecurity risks, but it may not be used consistently throughout the firm. Cybersecurity practices have become more formalized within the banking sector. Specific policies, procedures, and guidelines are documented and disseminated across the organization, ensuring that employees follow established protocols for handling cyber threats. However, although there is a structured approach to cybersecurity risk management, it may not be consistently applied across the entire banking operations.* |
| *Managed - 3* | *Cybersecurity practices are consistently implemented and monitored throughout the organization. There is a focus on continuous improvement and the use of metrics and key performance indicators to track progress and effectiveness of cybersecurity measures.* |
| *Optimized - 4* | *At the optimized level, cybersecurity practices are fully integrated into banks' overall business strategy and culture. There is a proactive approach to cybersecurity, security measures are no longer reactive but are strategically planned and implemented to anticipate future challenges with continuous optimization of processes and technologies to adapt to evolving threats and challenges.* |

*Table 4 - Maturity Levels*

# Chapter Five

# 5. Data Analysis

## 5.1 Overview

In this section, the analysis of the qualitative data collected through interviews is presented. The interview responses were analyzed using the steps of thematic analysis outlined in the research methodology section. The interview responses were reviewed, and based on the transcripts, the codes can be categorized into themes addressing the research questions. Six themes were identified from the responses to the interview questions. The identified themes were reviewed and defined so that they could align with the specific objectives of the study. These themes comprise maturity inconsistencies, framework applicability, existing framework deficiencies, inconsistent security practices, resource constraints, and the necessity for customization. Based on these themes, the participant's interview responses are described and analyzed as follows.

The main respondents were IT and CS directors in the selected banks. This method enables the researcher to obtain a high-level perspective of senior managers in cybersecurity maturity. Accordingly, interviews have been conducted with 12 IT/CS directors and professionals from 9 bank sectors. For confidentiality and ethics considerations of the research, the researcher has anonymized the name of banks as Bank-A to Bank-I throughout the analysis process.

## 5.1 Thematic Analysis

### 5.1.1 Familiarization with Collected Data

Analysis is facilitated by an in-depth knowledge of, and engagement with, the data set. [115] Familiarization involves reading and rereading transcripts, listening to audio-recordings, making notes of any initial annalistic observations. It helps the researcher to move the analysis beyond a focus on the most obvious meanings. The data collected from the banks were captured and notes were taken to make it easy and simple to understand the overall sense of challenges faced by the bank professionals and managers. [116] The thematic approach was utilized to qualitative data analysis and a method for detecting, analyzing, and reporting patterns (themes) within data. A theme is "something important about the data in relation to the research question and represents some level of patterned response or meaning from the data set.

### 5.1.2 Transcription of the Data

Transcription involves converting audio or video recordings into written text. This step ensures that the data can be analyzed systematically. Researchers typically transcribe interviews, focus

groups, or any verbal data into written form for easier reference [117]. After conducting the interviews with IT/CS manager and professionals, the researcher transcribers every record verbatims into readable texts for detailed analysis.

### 5.1.3 Coding

Coding is a systematic process of identifying and labelling relevant features of the data (in relation to the research question) and is the first step in the process of identifying patterns in the data because it groups together similar data segments. It also helps in identifying important features of the data that are relevant to the research question. It can be words or short phrases that represent key points in the text. [118] In this step, the researcher assigns labels (codes) to specific pieces of data. The codes, patterns/sum-themes and themes are attached as Annex C in a table format.

### 5.1.5 Define the Themes

Based on these themes, the participants interview responses are described and analyzed as follows.

#### Maturity Inconsistency

In the Ethiopian banking sector, there is a noticeable disparity in the level of cybersecurity maturity across selected banks. While few selected banks have begun to implement formalized cybersecurity processes, such as risk management and incident response protocols, others still operate with ad hoc practices, responding to cyber threats only when incidents occur. This lack of a standardized approach results in a fragmented cybersecurity landscape, where other banks are more vulnerable to threats due to the absence of consistent and institutionalized security frameworks. In particular, the limited training of bank staff regarding cybersecurity awareness further exacerbates these inconsistencies, making it difficult for banks to build a cohesive security culture [95]. This variation in cybersecurity maturity levels points to the need for a more uniform and structured approach across the banking sector, ensuring that all banks can adequately safeguard their information systems for breach, alter, and damage. In contrast, two IT/CS directors, when asked about their current security maturity level:

"*… we've tried to adopt C2M2 to measure our cybersecurity current state, and we are at MIL 3 (managed) level*".

### Framework Applicability

The adoption of international cybersecurity frameworks, such as ISO 2700, C2M2 and NIST CSF, within Ethiopian banks has been uneven. Larger banks with more resources are more likely to adopt these global standards, benefiting from their comprehensive risk management strategies and structured controls. However, many smaller or mid-sized banks struggle to implement these frameworks due to resource limitations, both in terms of budget and cybersecurity expertise [106]. While international frameworks offer a robust approach to cybersecurity governance, they are not always easily adaptable to the local context, where banks face specific challenges related to infrastructure and regulatory constraints.

To refer two of the respondent's response:

> "*... the investment we required to make to fully adopt ISO27001, our bank was asked to pay more than 30,000 USD as the bank was considered as a large business entity with complex banking systems. Moreover, it was quite complex for our IT and CS professionals to fully understand all the framework domains of ISO27001*".

In some cases, the international frameworks' focus on third-party risks and vendor management is underutilized, as many Ethiopian banks have not yet fully integrated these aspects into their cybersecurity strategies [103]. As a result, the applicability of these frameworks remains partial, highlighting the need for more contextually appropriate solutions.

### Existing Framework Deficiencies

The current cybersecurity frameworks implemented in Ethiopian banks exhibit significant gaps, particularly in addressing operational cybersecurity challenges like supply chain security, ATM security, and mobile money security. As operational banking platforms become more prevalent in Ethiopia, they present unique challenges that are often under-addressed by the existing frameworks. For instance, mobile banking applications are frequently targeted by fraudulent activities such as SIM swap attacks and unauthorized access, but the existing security measures are not sufficient to mitigate these threats [78]. The findings indicate that the awareness and understanding of cybersecurity maturity frameworks within Ethiopian banks are significantly limited, particularly considering the high level of risks associated with the banking sector. Although few selected banks possess a general understanding of their cybersecurity posture, most

of this awareness is restricted to cybersecurity professionals only. These professionals recognize the risks associated with not having a tailored assessment framework, yet broader awareness across the organization remains low.

Of the nine banks surveyed, only one had developed and implemented its own cybersecurity maturity assessment framework to evaluate its security posture and assess existing vulnerabilities. However, even this framework lacks the necessary uniqueness, as it largely replicates maturity capabilities and categories derived from international standards such as ISO 27001, NIST, and C2M2.

To quote the response from the CS director:

> "*Bank-c has its own in-house cybersecurity maturity model. We used C2M2 capability maturity model components as a reference. Yet, it doesn't address our need as it doesn't address some components*".

Additionally, when asked about being audited by external parties:

> "*No, we have not yet been able to invite auditors to measure the effectiveness of our maturity measures*".

This replication raises concerns about the true effectiveness of the framework, as it does not appear to be fully customized to meet the specific needs and context of the Ethiopian banking environment. This issue is compounded by inconsistent implementation of cybersecurity controls across departments, where some operational areas receive greater protection than others, leaving critical systems exposed. Without addressing these deficiencies, Ethiopian banks will remain vulnerable to cyberattacks, particularly as digital banking services expand [75].

### Inconsistent Security Practice

The lack of uniformity in cybersecurity practices across Ethiopian banks is a significant challenge. Different departments within the same institution often apply disparate levels of security controls, leading to uneven protection and gaps in the bank's overall cybersecurity posture. For instance, while certain operational units may adhere strictly to cybersecurity protocols and utilize proper

mechanisms for managing them, others rely on manual processes or outdated systems, delaying the bank's response to security threats [79]. This inconsistent application of security policies not only weakens the bank's defense against cyberattacks but also creates vulnerabilities that could be exploited by attackers.

To quote the response of three IT professionals:

> "*One of the major challenges we have in our bank is the absence of formal security implementation and responsible body to enforce that. Sometimes, policies are developed by other departments for the sake of fulfilling regulatory requirements like INSA*".

Policy enforcement varies between teams, with some departments exhibiting greater adherence to cybersecurity protocols than others. This fragmentation in security practices underscores the need for standardized controls and uniform policy enforcement across all departments to ensure comprehensive protection [76].

### Resource Constraints

The other pressing issues faced by the banking sector is the significant limitation of financial resources and cybersecurity expertise. Almost all selected banks for this research paper struggle to allocate sufficient budget for cybersecurity initiatives, which leads to delayed implementation of advanced security measures such as continuous monitoring systems, SIEM tools, and encryption technologies [36].

To refer few responses from three IT directors from Bank -B and one CS director from Bank-G:

> "… *we need extensive human capital to address emerging cybersecurity threats in banking sector. However, as the level of awareness among leaders is low, we are unable to get updated security know-how to protect our cyber space. As an option, although we recommend our management to hire consultants to adopt international frameworks, costs are very expensive to manage*".

The shortage of skilled cybersecurity professionals further exacerbates this problem, leaving many institutions reliant on understaffed IT departments to manage increasingly complex cyber risks. Additionally, the high cost of adopting cutting-edge technologies poses a barrier for smaller banks, preventing them from achieving the same level of cybersecurity maturity as their larger counterparts. Without the necessary investment in both human resources and technology upgrades, banks will continue to face difficulties in maintaining a robust cybersecurity posture [19].

### Necessity for Customization

Given the specific challenges faced by the banking industry, there is a clear need for a customized cybersecurity maturity framework that addresses the localized threats and regulatory requirements. While international frameworks provide a valuable foundation, they often fail to account for the resource limitations and unique cyber threats prevalent in the region.

To concrete the analysis, two respondents mentioned that"

> "*We have tried our best to assess our maturity by utilizing internal expertise, but it seems difficult to achieve it without investing a lot of money. So, we highly recommend having a contextualized or customized maturity assessment framework*".

For example, the banking sector faces particular risks related to the rapid expansion of digital financial services and the growing reliance on mobile banking, which are not sufficiently covered by the current frameworks [39]. Moreover, the regulatory landscape in Ethiopia, though evolving by introducing new regulations like CMCSRS, lacks the comprehensive guidance needed to support international frameworks fully. A tailored approach to cybersecurity would allow banks to implement scalable and resource-efficient solutions that align more closely with local needs, ensuring greater resilience against cyber threats and regulatory compliance [40].

# Chapter Six
# 6. Result and Discussion

The main aim of the study is to assess the existing cybersecurity maturity assessment frameworks in banks, review international standards, compare and analyze their possible gaps and limitations, and propose a customized framework that could address the identified gaps. Below, the discussions are explained in detail.

***RQ1**: What cybersecurity maturity assessment frameworks are available for use in the Ethiopian banking sector?*

The result of the study reveals that there is a significant gap in the development of the cybersecurity maturity assessment framework in the banking sector. The notion of having a tailored or customized in-house developed framework is quite minimal based on the analysis of 9 selected banks data. Out of 9 selected banks only 1 bank has shown the potential to create its framework to assess its own cyber space. Despite owning their assessment framework, through document analysis, we have identified that the framework is a copy-paste of well-known international standards like ISO27001 and C2M2. Moreover, the components that are listed in the frameworks are vague and complex, and don't address cybersecurity strategy and policy, awareness and culture development programs, mobile money security, data protection, supply chain security, and consider regulatory requirements. The bank failed to contextualize Ethiopian cyberspace, inconsiderate its banking cybersecurity challenges and capture specific operations.

The other 8 banks that have been examined in the study demonstrated that they don't own a cybersecurity maturity assessment framework. This indicates that there is a huge gap in their cybersecurity strategy and policy as they leave space for potential vulnerabilities. Without a tailored assessment framework, these banks are unable to value and improve their security posture, which is quite critical for their day-to-day operational activities. The dependency on high-level international standards coupled with the complete absence of a tailored framework indicates a critical issue in the banking sector. We collectively understand that the complete absence of a cybersecurity maturity assessment framework reflects a lack of awareness and culture development in the banking sector rather than a potential underestimation of existing cybersecurity risks. This result shows that having a tailored framework is essential to address existing cybersecurity challenges and threats.

***RQ2**: What are the limitations and positive aspects of existing cybersecurity maturity assessment frameworks, and how applicable are they in Ethiopian banks?*

While analyzing the similarities and differences among existing cybersecurity maturity assessment frameworks, the results have shown even though they can demonstrate a comprehensive way of managing cybersecurity risks, they failed to address specific cybersecurity challenges and risks that the banking sector is facing. We have picked up and analyzed international well-known cybersecurity maturity assessment frameworks like ISO 27001, NIST CSF, C2M2, COBIT 5, FAIR, CIS Controls, CIS RAM, HITRUST CFM, FSSCC Cybersecurity Controls, NICE Cybersecurity Framework, CRAMM, CERT-RMM, and SSE-CMM.

In analyzing their similarities, these frameworks are designed to provide a structured way/approach for assessing cybersecurity maturities, identifying risks, governance, and other issues. They also have common features such as components, control objectives, systematic risk management, and evaluations. In addition, they have worldwide enrichment as they can be implemented anywhere in the world. Regardless of their limitations and gaps, they can even be implemented in Ethiopian banking and other sectors. However, gap analysis shows that these cybersecurity maturity assessment standards have quite limitations considering the Ethiopian banking industry context, even if some banks tried to utilize them for assessing their security posture. Some of the limitations include:

- They failed to capture the needs and cybersecurity challenges faced by the banking sector,
- They are not easy to understand,
- They require huge investments to utilize by our banking sector,
- They don't incorporate Ethiopian regulatory requirements,
- They demand a highly skilled professional and expertise, which is quite rare in our context,
- The time they took to complete is extended and exhaustive sometimes,
- They have major differences in their nature such as:
    - COBIT 5: focus on audit, compliance, and IT service governance,
    - SSE – CMM: focus on engineering disciplines,

- FAIR: focus risk management,
- CERT – RMM: focus on cyber resilience.

Trying to utilize these frameworks as is, without customization, may result in an unaligned cybersecurity understanding. Even if they provide an outstanding foundation in the realm, their lack of concentration in the banking sector in Ethiopia comprises regulatory compliance, financial and personal data protection, and the risk appetite that the banks have. Additionally, we have identified quite unrealistic results of cyber maturity levels after utilizing international standards such as ISO27001, C2M2, and NIST CSF. To summarize, even if these international standards are valuable and icebreakers for current developments, they require visible adaptation to be fully applicable in our banking sector.

***RQ3**: What innovative solution be tailored to address the specific needs and challenges of the Ethiopian banking sector while incorporating the best practices of existing cybersecurity maturity frameworks?*

To address the specific needs and challenges of the Ethiopian banking sector, customized, innovative cybersecurity maturity assessment framework that goes beyond the existing international standards has been proposed. The new proposed framework doesn't only incorporate the best practices from well-known standards such as ISO 27001, C2M2, and GDPR but also tailors its approach by introducing components that fit the purpose of the operational banking environment. It also addresses the gaps identified in the current cybersecurity landscape.

The key element of the proposed framework is regulatory compliance, which mainly focuses on creating alignment with existing legislation and regulations introduced by the National Bank of Ethiopia (NBE). The critical NBE directives related to IT and/or CS initiative "Requirements for Information Technology (IT) Management of Banks Directive No. SBB|83|2022" has clearly indicated that banks should comply with the requirements of Management of IT Risks, IT Risk Management Policies, Automation of Core Business Processes, Training and Awareness, and IT Audit. The best part of this key element is not only forcing banks to strategically comply with the key requirements but also helping them to mitigate legal and regulatory risks. Furthermore, banks as a critical financial sector for the country are obliged to comply with the minimum requirements of the Critical Mass Cyber Security Requirements Standard (CMCSRS). This mandatory

requirement standard has contextualized cybersecurity capability buildings and processes that help the banking sector to at least address its components.

To make it easier for banks to consider, the proposed framework also incorporates the notion of mobile money security which reflects the fastest growing trend in the Ethiopian banking sector. Considering the adoption of mobile money services in the country, the component specifically addresses vulnerabilities associated with financial transactions using mobiles. The component has minimum security controls like authentication, encryption, secure development, and fraud detection to ensure customers can confidently use banking services without disruption and data loss. In addition to that, supply chain security has been added as an innovative component by recognizing the connective nature of modern banking operations and is mainly concerned with identifying risks associated with third-party suppliers and partners. The component helps the bank to prevent breaches resulting from supply chain attacks through implementing security controls such as vendor assessment, placing contractual agreements, and monitoring.

Moreover, the proposed framework has introduced awareness and culture development components to create a robust cyber-conscious culture. This component concerns creating a sectorial culture to equip all banking employees to be active players in this virtual reality and mainly focuses on cyber education, training and awareness, and cyber literacy. The main objective of incorporating this component is to avoid risks that arise from human errors. Additionally, personal data protection is also a key ingredient part of the whole framework and aims to safeguard personal and financial consumer data from alteration, breach, and damage. As a best practice, the framework suggests that the banking sector could learn (utilize the principles and data subject rights) from the General Data Protection Regulation (GDPR) to make it well organized. Furthermore, Ethiopia has recently introduced a new Personal Data Protection Proclamation No. 1321/2024 that supports the component ideas.

Finally, business continuity and disaster recovery, incident response planning, and other components are included in the proposed framework. By integrating these components, this framework offers a simple, innovative, and tailored solution for the specific needs of the Ethiopian banking sector. It doesn’t only meet national regulatory requirements but also addresses international best practices and meets global standards.

***RQ4**: What metrics or mechanisms can be used to measure the effectiveness of the proposed framework in achieving its intended outcomes?*

The proposed cybersecurity maturity assessment framework tailored for the Ethiopian banking sector has proven to be an effective tool as it went through an expert review validation. The framework design: graphical illustration and detailed explanation, incorporating multiple controls, international best practices, and regulatory compliance aligned with the specific needs of the banking sector. The validators have rigorously highlighted its contextualized notion of integrating local regulatory compliance, cultural considerations, and its unique operational challenges faced by the banks sector. They also mentioned that the framework reveals key strengths as it focuses on addressing the limitations and gaps identified by the international standards when implemented or applied to the Ethiopian context. Their review assures the framework effectively captures the nuances of the banking sector that are more often overlooked by the generic frameworks. Furthermore, the framework introduced components such as awareness and culture development programs, supply chain security, mobile money security, ATM security, personal data protection, and BC and DR, and the experts emphasized these elements are underrepresented in traditional frameworks. To summarize, the expert review has affirmed that this contextualized cybersecurity maturity framework is a highly effective tool for the Ethiopian banking sector. Starting from its ability to measure cybersecurity maturity accurately to its potential to make an asset for banks to consider as an enhancement tool for their cybersecurity programs.

## 6.1 Framework Evaluation Result

To validate the effectiveness of the proposed cybersecurity maturity assessment framework, expert review is a widely accepted method in academic research. This process involves obtaining feedback from domain experts to assess the framework's relevance, feasibility, completeness, and applicability to the intended context [114]. In the case of the cybersecurity maturity assessment framework designed for the banking industry, a structured expert review process provided insightful feedback, validated assumptions, and identified areas for improvement. The method ensures that the framework is aligned with industry standards and is feasible for implementation in real-world settings.

### 6.1.1 Selection of Experts

To maintain objectivity and relevance, the expert panel consists of 3 cybersecurity professionals, each with a minimum of 10 years of experience in cybersecurity domain. The experts include

cybers governance and management director, senior cybersecurity advisor, and cybersecurity project manager from both public and private banking institutions. Moreover, all of the experts are CISM certified which makes them ideal candidate to review and validate the effectiveness of the proposed framework. To be ethical and confidentiality issues, the names of these experts is anonymized as Expert – A, Expert - B, and Expert – C.

### 6.1.2 Framework Presentation

The experts were provided with a detailed document outlining the structure (illustration), components, sub-components, and controls of the proposed cybersecurity maturity assessment framework designed for the banking industry. The presentation highlighted how the fit the purpose of banking sector.

### 6.1.3 Evaluation Criteria and Feedback

The experts were asked to evaluate the framework based on the following four criteria: relevance, feasibility, completeness and consistency, and flexibility. Below is a summary of each expert's evaluation:

- **Relevance**: Expert - A reviewed the relevance of the proposed framework and commented as "*the framework is highly relevant to the banking industry as it's crucial to manage evolving cybersecurity threats related to the banking industry. Especially, the point where the framework addressed the rise of mobile banking threats, ATM attacks, and supply chain risk management. These inclusions demonstrate a clear understanding of the challenges the banking sector faces*". In the same vein, Expert – B emphasized supply chain security and praised the focus on vendor assessment and contractual obligations as essential for managing risks arising from external parties. Whereas Expert – C suggest the framework should focus should be on operational continuity as "… the framework will be more relevant when it particularly addresses operational controls such as network security and incident response rather than managerial aspects".
- **Feasibility**: regarding the framework feasibility, Expert - A has raised concerns about the implementation advanced controls as *"... some of the framework controls such as SIEM tools and real-time fraud detection algorithms may be challenging for small sized banks with limited resource. The expert suggests tiering the controls based on the bank size and operational complexity*". In another vein, Expert – B demonstrated doubt on the

implementation timelines as they could be challenging for resource intensive components i.e., real-time fraud monitoring, and suggested "it would be better if the framework incorporate phased implementation to ease the process". Expert – C, like Expert – A focused on the challenges that small-sized banks have and the upfront investment it requires to implement.

- **Completeness & consistency**: on the other hand, the Expert - A suggests the inclusion of additional controls and alignment with existing frameworks as "*the framework is well-aligned with industry standards and admired the framework's strong focus on personal data protection and regulatory compliance*". Concerning the completeness of it, the expert recommends the integration of cloud security controls, as more banks are migrating to cloud-based infrastructure. Additionally, Expert – B also support having post-incident analysis and lesson learned in IRP domain. Expert – C, in the other hand raised a concern as "… instead of having cryptography as a domain, it would be better to incorporate in network security domain as a sub-domain as they have quite similar behaviors".

- **Flexibility**: both Expert – A and B finds the framework adaptable to both large and medium-sized banks. However, insisted, the framework should provide scalable recommendation for small-sized banks due to their resource shortages. Whereas Expert – C put his suggestion as "*creating industry specific variations to allow for differences in regulatory requirements across region. This would make the framework more adaptable for other institutions*".

The findings of the evaluation showed that the proposed cybersecurity maturity assessment framework is being accepted and valid to help the banking sector to identify their security posture and manage security risks. However, the proposed framework should be evaluated through practical application and more research conducted so that it can be modified and enhanced over time.

# Chapter Seven
# 7. Summary and Future work

This chapter presents the conclusion and recommendation of the study. The conclusions are derived from the research findings. Its focus is on showing how the result relates to the original research question and objective set out in the thesis. The chapter also provides recommendations that have emerged from this study.

## 7.1 Summary

This research manuscript proposed a contextualized and customized cybersecurity maturity assessment framework for the Ethiopian banking sector. The proposed framework has considered current cybersecurity challenges the banking sector faces, international standards, as well as national regulatory frameworks. This framework is presented to the banks to self-assess their cyberspace to measure the security levels. Subsequently, identifying their exact security posture, addressing their limitations, and developing mitigation plans and continuous improvement.

To build a customized maturity framework for the Ethiopian banking sector, we studied the current cybersecurity frameworks followed by the selected banks. Furthermore, we investigated and compared recent international cybersecurity maturity frameworks to identify their limitations. Therefore, all the defined cybersecurity maturity assessments have defined *11 domains*, *43 subdomains*, and *94 controls* to be implemented. The implementation of the controls by the banks ranged among five maturity levels: Ad hoc, Initial, Defined, Managed, and optimized. Each maturity level in each domain has a clear and precise description displayed to the banking industry which they need to confirm after implementation. The validation process, involving expert review, has strengthened the framework's credibility and applicability in real-world scenarios. This approach has ensured that the framework aligns with industry best practices, regulatory requirements, and the evolving threat landscape faced by banks.

Additionally, the proposed framework should always be enhanced from time to time to adapt to the new regulatory requirements, cyber threats, and mechanisms. It also contributes significantly to the field of cybersecurity in banking, offering a practical assessment tool for banks to enhance their resilience against cyber threats. By implementing this framework, banks can better protect sensitive data, maintain operational continuity, and safeguard customer trust in an increasingly digital financial ecosystem.

In conclusion, this thesis presents a valuable contribution to the critical domain of cybersecurity in banking, offering a validated framework that can help financial institutions navigate the complex and ever-evolving landscape of cyber threats.

## 7.2 Recommendation and Future Work

While this research provides a solid foundation for cybersecurity maturity assessment in banking, future studies could explore the framework's long-term impact on security outcomes and its adaptability to emerging technologies such as AI and IoT and threats. Additionally, it can be improved by allowing the banks to publish their cybersecurity maturity levels after utilizing this framework. Also, the framework can be automated to address all bank entities easily and efficiently. For future work, the framework can be enhanced to be accurately mapped with national standards like CMCSRS as a preliminary step for banks to become certified. In terms of maturity requirements, the framework doesn’t include trending domains like IoT and AI. Moreover, the proposed framework can also be adapted to be applied to different sectors other than the banking industry, such as critical infrastructure and peace and security sectors.

## References


[1] KPMG, “A socio-technological analysis of cybercrime and cyber security in Nigeria,” *ISACA Annu. Kenya Conf. - Secure Kenya II Nairobi*, 2015.

[2] Halefom Hailu, “The state of cybercrime governance in Ethiopia,” Artic. Publ. Res., 2015, [Online]. Available: available at https://www. researchgate.net/publication/322234805_THE_STATE_OF_CYBERCRIME_GOVERNANCE_ IN_ETHIOPIA, 2015.

[3] Verizon, “2021 Data Breach Investigation Report,” *Verizon Enterprise*, 2021.

[4] Trend, “Ransomware in Banking Sector Skyrockets in 2021,” *Trend Micro*, 2021.

[5] Kaspersky, “Financial Institutions Security Risk Report,” *Kaspersky Lab*, 2019.

[6] IBM, “Cost of Insider Threats Global Report 2020,” *IBM Security.*, 2020.

[7] Ponemon, “2021 third-party Risk Study,” *Ponemon Inst.*, 2021.

[8] MaAfee, “2020 Mobile Threat Report,” *McAfee Labs*, 2020.

[9] EAST, “European Association for Secure Transactions ATM Fraud Report,” 2020.

[10] KPMG, “Data Protection, Privacy and Cybersecurity,” *ISACA Annu. Kenya Conf. - Secure Kenya II Nairobi*, 2015.

[11] Ouma, Derick O., “A Cybersecurity Maturity Model and Toolkit for self-assessment,” *O Ouma Cybersecurity Matur. Model Toolkit Self-Assess. Univ. Nairobi*, pp. 5-7, 2021.

[12] Shimels, Tadele and Lessa, Lemma, “Maturity of information systems’ security in Ethiopian banks: case of selected private banks,” *Int. J. Ind. Eng. Oper. Manag.*, 2023.

[13] K. Abate, Misrak Tesfaye Ratinder, “Banking sector in Ethiopia: Origin and present state,” *EPH-Int. J. Bus. Manag. Sci.*, vol. 9, pp. 4--8, 2023, doi: https://doi.org/10.53555/eijbms.v9i2.134.

[14] O. Reis, O. Obi, F. Osasona, and J. Oliha, “CYBERSECURITY DYNAMICS IN NIGERIAN BANKING: TRENDS AND STRATEGIES REVIEW.,” *Comput. Sci. IT Res. J.*, vol. 5(2), pp. 336–364, 2024.

[15] A. J. S. Rojas, J. Armas-Aguirre, E. F. P. Valencia, and J. M. M. Molina, “Cybersecurity maturity model for the protection and privacy of personal health data.,” Nov. 2022, [Online]. Available: https://doi.org/10.1109/icalter57193.2022.9964729

[16] A. Aborujilah, A. Z. Al-Othmani, N. S. Hussien, S. A. Mokhtar, Z. A. Long, and M. Nizam, “Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian

Universities as Case Study," in *2022 9th International Conference on Electrical and Electronics Engineering (ICEEE)*, 2022, pp. 440–450. doi: 10.1109/ICEEE55327.2022.9772546.

[17] Aliyu, Aliyu and Maglaras, Leandros and He, Ying and Yevseyeva, Iryna and Boiten, Eerke and Cook, Allan and Janicke, Helge, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Appl. Sci.*, vol. 20, p. 2660, 2020.

[18] Almomani, Iman and Ahmed, Mohanned and Maglaras, Leandros, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, 2021.

[19] Abebe G., "A framework for human factors influence on information systems security at commercial banks in Ethiopia," *MSc Thesis Addis Ababa Univ. Unpubl.*, 2020.

[20] Shirley Radack, "Managing information security risk: organization, mission, and information system view," *US Spec. Publ. 800 - 36*, 2011.

[21] Rabii, Anass, Saliha Assoul, Khadija Ouazzani Touhami, and Ounsa Roudies, "Information and cyber security maturity models: a systematic literature review," *Emerald Publ. Ltd.*, 2020.

[22] A. Hassan, A. Abdul, S. Dawodu, S. Ewuga, M. Oladeinde, and T. Abrahams, "CYBERSECURITY IN BANKING: A GLOBAL PERSPECTIVE WITH A FOCUS ON NIGERIAN PRACTICES.," *Comput. Sci. IT Res. J.*, vol. 5(1), pp. 41–59, 2024.

[23] Munirul, Ula and Zuraini, Ismail and Zailani, S Mohamed, "A Framework for Governance of Information Security In Banking Systems," 2011.

[24] Working group for information systems security for the banking and financial sector, "Information systems audit policy for the banking and financial sector," 2001.

[25] "Oxford University Press. 2014. Oxford Online Dictionary," 2014, [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity

[26] Craigen, Dan and Diakun-Thibault, Nadia and Purse, Randy, "Defining cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, 2014.

[27] Rea-Guaman, Angel Marcelo and San Feliu, Tom{\'a}s and Calvo-Manzano, Jose A and Sanchez-Garcia, Isaac Daniel, "Comparative study of cybersecurity capability maturity models," *Softw. Process Improv. Capab. Determ. 17th Int. Conf. SPICE*, pp. 100--113, 2017.

[28] G. Emily and K. Shankar, “Cybersecurity Threats Targeting Networked Critical Medical Devices,” Purdue University, Aug. 2018. doi: 10.5703/1288284316840.

[29] N. O’Brien *et al.*, “Usability and Feasibility Evaluation of a Web-Based and Offline Cybersecurity Resource for Health Care Organizations (The Essentials of Cybersecurity in Health Care Organizations Framework Resource): Mixed Methods Study,” *JMIR Form Res*, vol. 8, p. e50968, Apr. 2024, doi: 10.2196/50968.

[30] P. L. Bowen, M.-Y. D. Cheung, and F. H. Rohde, “Enhancing IT governance practices: A model and case study of an organization’s efforts,” *Int. J. Account. Inf. Syst.*, vol. 8, no. 3, pp. 191–221, 2007, doi: https://doi.org/10.1016/j.accinf.2007.07.002.

[31] H. M. Alzoubi *et al.*, “Cyber Security Threats on Digital Banking,” in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, pp. 1–4. doi: 10.1109/ICAIC53980.2022.9896966.

[32] R. S. Rao and A. R. Pais, “Detection of phishing websites using an efficient feature-based machine learning framework,” *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3851–3873, Aug. 2019, doi: 10.1007/s00521-017-3305-0.

[33] R. Butler and M. Butler, “Assessing the information quality of phishing-related content on financial institutions’ websites,” *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 514–532, Jan. 2018, doi: 10.1108/ICS-09-2017-0067.

[34] N. N. Neto, S. Madnick, A. M. G. D. Paula, and N. M. Borges, “Developing a Global Data Breach Database and the Challenges Encountered,” *J Data Inf. Qual.*, vol. 13, no. 1, Jan. 2021, doi: 10.1145/3439873.

[35] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, and S. A. Ebad, “Cyber Threats Classifications and Countermeasures in Banking and Financial Sector,” *IEEE Access*, vol. 11, pp. 125138–125158, 2023, doi: 10.1109/ACCESS.2023.3327016.

[36] Amare, B, “Assessment of insider threat in Ethiopian banking industry,” *Thesis Work Addis Ababa Univ. Addis Ababa*, 2015.

[37] S. Prabhu and N. Thompson, “A primer on insider threats in cybersecurity,” *Inf. Secur. J. Glob. Perspect.*, vol. 31, no. 5, pp. 602–611, 2022, doi: 10.1080/19393555.2021.1971802.

[38] E. B. Beshah, “An Investigation on the Current Information System Security Maturity Level of the Banking Industry in Ethiopia.,” *Addis Ababa Univ.*, pp. 8--9, 2017.

[39] Tebkew, Kelemie, “Information Security Management Framework For Banking Industry In Ethiopia,” *Thesis Work Addis Ababa Univ. Addis Ababa*, 2013.

[40] Negussie, Abeselom, “Practices, challenges and prospects of information security policy in Ethiopian banking industry,” *Addis Ababa Univ.*, 2015.

[41] I. Mohammed and A. Musa Bade, “CYBERSECURITY CAPABILITY MATURITY MODEL FOR NETWORK SYSTEM,” *Int. J. Dev. Res.*, vol. 09, pp. 28637–28641, Jul. 2019.

[42] A. Garba, M. Sirat, and S. Othman, “An Explanatory Review on Cybersecurity Capability Maturity Models,” *Adv. Sci. Technol. Eng. Syst. J.*, vol. 5, pp. 762–769, Aug. 2020, doi: 10.25046/aj050490.

[43] M. Bada and W. H. Caroline, “Cybersecurity Capacity Review Republic of Lithuania,” *Available at SSRN 3658453*, 2017.

[44] E. Nagyfejeo, H. Weisser, and Caroline, “Cybersecurity Capacity Review Former Yugoslav Republic of Macedonia (FYR Macedonia),” *Available SSRN*, Jul. 2018, [Online]. Available: https://ssrn.com/abstract=3658462 or http://dx.doi.org/10.2139/ssrn.3658462

[45] K. Muronga, M. Herselman, A. Botha, and A. Da Veiga, “An Analysis of Assessment Approaches and Maturity Scales used for Evaluation of Information Security and Cybersecurity User Awareness and Training Programs: A Scoping Review,” in *2019 Conference on Next Generation Computing Applications (NextComp)*, 2019, pp. 1–6. doi: 10.1109/NEXTCOMP.2019.8883535.

[46] A. Woretaw, L. Lessa, and S. Negash, “Factors Hindering Full-Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture,” Jul. 2019.

[47] T. Bagh, M. A. Khan, T. Azad, S. Saddique, and M. A. Khan, “The Corporate Social Responsibility and Firms’ Financial Performance: Evidence from Financial Sector of Pakistan,” *Int. J. Econ. Financ. Issues*, vol. 7, no. 2, pp. 301–308, 2017.

[48] K. Wong, “The Hackers and Computer Crime against Financial Institutions,” *EDPACS*, vol. 14, no. 5, pp. 1–7, 1986, doi: 10.1080/07366988609450384.

[49] J. G. Alayo, P. N. Mendoza, J. Armas-Aguirre, and J. M. Molina, “Cybersecurity maturity model for providing services in the financial sector in Peru,” in *2021 Congreso*

*Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, 2021, pp. 1–4. doi: 10.1109/CONIITI53815.2021.9619733.

[50] El ghazi El Houssa{\"\i}ni, Souha{\"\i}l and Youssfi, Karim and Boutahar, Jaouad, "CAT5: a tool for measuring the maturity level of information technology governance using COBIT 5 framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, 2016.

[51] M. Battaglioni, G. Rafaiani, F. Chiaraluce, and M. Baldi, "MAGIC: A Method for Assessing Cyber Incidents Occurrence," *IEEE Access*, vol. 10, pp. 73458–73473, 2022, doi: 10.1109/ACCESS.2022.3189777.

[52] ISO27001:2022, "Information technology – Security techniques – Information security management systems – Requirements ,." International Organization for Standardization, Geneva, ISO/IEC 27001 2022.

[53] F. Djebbar and K. Nordström, "A Comparative Analysis of Industrial Cybersecurity Standards," *IEEE Access*, vol. 11, pp. 85315–85332, 2023, doi: 10.1109/ACCESS.2023.3303205.

[54] Almuhammadi, Sultan and Alsaleh, Majeed, "Information security maturity model for NIST cyber security framework," *Comput. Sci. Inf. Technol. CS IT*, vol. 7, pp. 51--62, 2017.

[55] N. Y. Center for Internet Security, "CIS Controls v7.1. Center for Internet Security," 2019, [Online]. Available: https://www.cisecurity.org

[56] N. National Institute of Standards and Technology, "Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. U.S. Department of Commerce," 2013, [Online]. Available: https://csrc.nist.gov

[57] Center for Internet Security (CIS), "CIS Risk Assessment Method (CIS RAM). Center for Internet Security.," *Cent. Internet Secur.*, 2018, [Online]. Available: https://www.cisecurity.org

[58] Butkovic, Matthew J and Caralli, Richard A, "Advancing cybersecurity capability measurement using the CERT{\textregistered}-RMM maturity indicator level scale," 2013.

[59] R. A. Caralli, J. H. Allen, P. D. Curtis, D. W. White, and L. R. Young, "CERT{\textregistered} resilience management model, version 1.0," *Softw. Eng. Inst.*, 2020.

[60] Hefner, R and Monroe, W, "System security engineering capability maturity model," *Conf. Softw. Process Improv.*, pp. 137--145, 1997.

[61] Axelos, "ITIL Foundation: ITIL 4 Edition," *Axelos Ltd. Lond.*, 2019.

[62] Newhouse, William and Keith, Stephanie and Scribner, Benjamin and Witte, Greg, "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," *NIST Spec. Publ.*, vol. 800, p. 181, 2017.

[63] Bitzer, Michael and H{\"a}ckel, Bj{\"o}rn and Leuthe, Daniel and Ott, Joshua and Stahl, Bastian and Strobel, Jacqueline, "Managing the Inevitable--A Maturity Model to Establish Incident Response Management Capabilities," *Comput. Secur.*, vol. 125, 2023.

[64] White, Gregory B, "The community cyber security maturity model," *2011 IEEE Int. Conf. Technol. Homel. Secur. HST*, pp. 173–178, 2011.

[65] Christopher, Jason D and Gonzalez, Dale and White, David W and Stevens, J and Grundman, J and Mehravari, N and Dolan, T, "Cybersecurity capability maturity model (C2M2)," *Dep. Homel. Secur.*, pp. 1–76, 2014.

[66] C. HITRUST, "HITRUST Alliance.," vol. V9.3, 2019, [Online]. Available: https://hitrustalliance.net

[67] PCI Security Standards Council, "PCI Data Security Standard (PCI DSS) v3.2.1.," *PCI Secur. Stand. Counc.*, 2018, [Online]. Available: https://www.pcisecuritystandards.org

[68] Financial Services Sector Coordinating Council (FSSCC)., "Cybersecurity Profile for Financial Institutions," 2018, [Online]. Available: https://www.fsscc.org

[69] J. Clark, A. Santos, and M. Weiss, "Financial services cybersecurity framework," *Evol. Landsc. J. Financ. Regul.*, vol. 8(1), pp. 45–67, 2019.

[70] Federal Financial Institutions Examination Council (FFIEC), "Federal Financial Institutions Examination Council (FFIEC)," *Cybersecurity Assess. Tool*, 2015, [Online]. Available: https://www.ffiec.gov

[71] R. A. Rothrock, J. M. Kaplan, and F. Van Der Oord, "The cyber threat landscape for financial institutions.," *Harv. Bus. Rev.*, vol. 2, pp. 67–81, 2018.

[72] B. Kurey and A. Arora, "Cybersecurity management in financial institutions: Challenges and solutions.," *Cybersecurity Rev.*, vol. 5(2), pp. 29–35, 2020.

[73] Kebede A., "Designing a framework for selecting effective information security awareness delivery method," *MSc Thesis Addis Ababa Univ. Unpubl.*, 2019.

[74] G. Terefe and D. Belay, "Evaluate the implementation of mobile banking security protocols in Ethiopia," *Addis Ababa Univ.*, 2020.

[75] E. Gera, “Assessment of maturity level of information security management using ISO 27002 at hospitals in Addis Ababa, Ethiopia,” *MSc Thesis Addis Ababa Univ. Unpubl.*, 2019.

[76] Nebyou Ejerssa, “Assessment of information security maturity level on Ethiopian public universities,” *MSc Thesis Addis Ababa Univ. Unpubl.*, 2018.

[77] B. Deferew, “Assess cyber hygiene practices among employees of Ethiopian commercial banks.,” *MSc Thesis Addis Ababa Univ. Unpubl.*, 2020.

[78] T. Deferew, “Examine the cybersecurity preparedness of Ethiopian banks,” *MSc Thesis Addis Ababa Univ. Unpubl.*, 2020.

[79] Yohannes, T., Lessa, L. and Negash, S. (, “Information security incident response management in an Ethiopian bank: a gap analysis,” *AMCIS*, 2019.

[80] G. Alemu and M. Girma, “Analyze the role of regulatory frameworks in digital financial services,” *MSc Thesis Addis Ababa Univ. Unpubl.*, 2021.

[81] M. Bahmanabadi and J. Edalatian Shahriari, “Evaluating the Maturity of Information Technology Governance in National Library and Archives of Iran, based on the COBIT 5 Framework,” *Iran. J. Inf. Process. Manag.*, vol. 37, no. 4, pp. 1096–1067, 2022, doi: 10.35050/JIPM010.2022.003.

[82] Sabillon, Regner and Serra-Ruiz, Jordi and Cavaller, Victor and Cano, Jeimy, “A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM),” *2017 Int. Conf. Inf. Syst. Comput. Sci. INCISCOS*, pp. 253--259, 2017.

[83] R. M. Adler, “A dynamic capability maturity model for improving cyber security,” in *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 2013, pp. 230–235. doi: 10.1109/THS.2013.6699005.

[84] Miron, Walter and Muita, Kevin, “Cybersecurity capability maturity models for providers of critical infrastructure,” *Technol. Innov. Manag. Rev.*, vol. 4, 2014.

[85] Akinsanya, Opeoluwa Ore and Papadaki, Maria and Sun, Lingfen, “Towards a maturity model for health-care cloud security (M2HCS),” *Inf. Comput. Secur.*, vol. 28, 2020.

[86] Mbanaso, Uche M and Abrahams, Lucienne and Apene, Oghenevovwero Zion, “Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework,” *Afr. J. Inf. Commun.*, vol. 23, pp. 1–26, 2019.

[87] M. Adimekwe, “Research Design,” 2024, pp. 267–287. doi: 10.1007/978-3-031-65749-8_5.

[88] T. Köhler, M. Rumyantseva, and C. Welch, “Qualitative Restudies: Research Designs for Retheorizing,” *Organ. Res. Methods*, Dec. 2023, doi: 10.1177/10944281231216323.

[89] B. Lunen, D. Hankemeier, and C. Welch, “Types of Research Design,” 2024, pp. 11–21. doi: 10.4324/9781003524113-2.

[90] S. McCombes, “Descriptive research design”, [Online]. Available: https://www.scribbr.com/author/shona

[91] V. Papakitsou, “Qualitative Research: Narrative approach in sciences,” *Dialogues Clin. Neurosci. Ment. Health*, vol. 3, no. 1, pp. 63--70, 2020.

[92] R. E. Roberts, “Qualitative Interview Questions: Guidance for Novice Researchers.,” *Qual. Rep.*, vol. 25(9), 2020.

[93] M. Nii Laryeafio and O. C. Ogbewe, “Ethical consideration dilemma: systematic review of ethics in qualitative data collection through interviews,” *J. Ethics Entrep. Technol.*, vol. 3, no. 2, pp. 94–110, Jan. 2023, doi: 10.1108/JEET-09-2022-0014.

[94] F. M. Leta, “Navigating the Moral Compass: Business Ethics in the Banking Sector,” *In Proceedings of the International Conference on Business Excellence*, pp. 311–320, 2024.

[95] M. Sharma and R. Trivedi, “Cloud computing security risks in the financial sector,” *J. Cloud Comput.*, vol. 9, pp. 30–43, 2020.

[96] S. Furnell and N. Clarke, “Effective cybersecurity education: Aligning knowledge with practice,” *Int. J. Cybersecurity*, vol. 5(2), pp. 45–52, 2012.

[97] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cybersecurity awareness campaigns: Why do they fail to change behavior?,” *Commun. ACM*, vol. 3, pp. 22–28.

[98] P. Pusey and W. Sadera, “The importance of cybersecurity certifications for career development,” *Cybersecurity Rev.*, pp. 38–42, 2011.

[99] SANS Institute, “The Value of Cybersecurity Certifications,” 2020, [Online]. Available: https://www.sans.org

[100] K. Evans and F. Reeder, “A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters.,” *CSIS Rep.*, 2010.

[101] House of People Representative, “Personal Data Protection Proclamation No. 1321/2024.” Negarit Gazette, 2024. [Online]. Available:

https://lawethiopiacomment.wordpress.com/wp-content/uploads/2024/08/personal-data-protection-proclamation-no.-1321-2024_signed-1.pdf

[102] B. Alotaibi, M. Zohdy, and M. Tahar, “A comprehensive framework for preventing phishing attacks in mobile banking,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, pp. 42–48, 2019.

[103] B. Pikas and M. Senn, “Managing third-party cyber risk in the financial sector.,” *J. Financ. Regul. Compliance*, pp. 32–46, 2016.

[104] M. Souppaya and K. Scarfone, “Guide to Cyber Threat Information Sharing (NIST SP 800-150),” *Natl. Inst. Stand. Technol.*, 2015, [Online]. Available: https://nvlpubs.nist.gov

[105] D. Shackleford, “The State of Cybersecurity Information Sharing: Data, Automation, and Analysis,” *Inst.*, 2016.

[106] N. Kshetri, “The Economics of Cybersecurity: A Practical Framework for Identifying and Dealing with Cyber Risk.,” *Springer.*, 2017.

[107] Information Network Security Administration, “Critical Mass Cyber Security Requirement Standard (CMCSRS) V2,” *Standard*, 2022, [Online]. Available: https://www.insa.gov.et/web/guest/ሰነዶች

[108] House of People Representative, “Computer Crime Proclamation No. 958/2016,” *Negarit Gaz.*, 2018, [Online]. Available: http://laws.eag.gov.et/Upload/CassationDecisionsDocument/992fbd9d-2fbb-40d2-9a62-7d5bb70b38fb.pdf

[109] National Bank of Ethiopia, “Requirements for Information Technology (IT). Management of Banks Directive No. SBB/83/2022,” *Natl. Bank Ethiop. Publ.*, 2022, [Online]. Available: https://nbe.gov.et/wp-content/uploads/2023/09/SBB-83-2022.pdf

[110] P. Voigt and A. Von Dem Bussche, “The eu general data protection regulation (gdpr).,” *Springer Int. Publ.*, vol. 1st, 2017.

[111] G. Almeida Teixeira, M. Mira da Silva, and R. Pereira, “The critical success factors of GDPR implementation: a systematic literature review,” *Digit. Policy Regul. Gov.*, vol. 21, no. 4, pp. 402–418, Jan. 2019, doi: 10.1108/DPRG-01-2019-0007.

[112] Y. Zhang, T. Wang, and C. Hsu, “The effects of voluntary GDPR adoption and the readability of privacy statements on customers’ information disclosure intention and trust,” *J. Intellect. Cap.*, vol. 21, no. 2, pp. 145–163, Jan. 2020, doi: 10.1108/JIC-05-2019-0113.

[113] Z. Georgiopoulou, E.-L. Makri, and C. Lambrinoudakis, “GDPR compliance: proposed technical and organizational measures for cloud provider,” *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 665–680, Jan. 2020, doi: 10.1108/ICS-01-2020-0009.

[114] A. Alenezi, H. F. Atlam, and G. B. Wills, “Experts reviews of a cloud forensic readiness framework for organizations,” *J. Cloud Comput.*, vol. 8, no. 1, p. 11, Aug. 2019, doi: 10.1186/s13677-019-0133-z.

[115] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual. Res. Psychol.*, pp. 77–101, 2006.

[116] M. Ruth, T. H. Michael, M. Bird, and B. Joan, “Approaches to Analysis of Qualitative Research Data: A Reflection on the Manual and Technological Approaches,” *Account. Finance Gov. Rev.*, vol. 27, 2021.

[117] C. Davidson, “Transcription: Imperatives for qualitative research,” pp. 35–52, 2009.

[118] J. Saldana, “The Coding Manual for Qualitative Researchers,” *Sage Publ.*, 2016.

# Appendix

## Appendix A: Interview questions

**Interview Questions and Questionnaires**

1. **Management questions**

    1. Could you describe the cybersecurity strategies that your bank is setting to manage cybersecurity risks?
    2. Does your bank have a formal cybersecurity maturity assessment framework?
    3. How do you assess your cybersecurity posture and measure progress? Or is there an in-house developed framework that aims to assess your institution's cybersecurity maturity level?
    4. If there is not in-house developed CMAF, what kind of international CMAF do you employ to assess your cybersecurity maturity level? e.g., ISO27001, NIST CSF, CMMI, COBIT …)?
    5. What are the biggest challenges that you face while implementing your CMAF?
    6. What are the challenges you face for not having or implementing CMAF?
    7. Who is responsible for implementing cybersecurity assessment framework within your institution?

2. **Domain Expert Questions**

    - General information
        - Name: _____
        - Organization: _____
        - Department: _____
        - Position: _____
        - Years of experience: _____

    - Are you familiar with your institution's current cybersecurity maturity assessment framework?
        - [ ] Yes [ ] No
    - If yes, which framework is being used?
        - NIST CSF [ ]

- ITIL [ ]
- CMMI (Capability Maturity Model Integration) [ ]
- COBIT (Control Objectives for Information and Technology) [ ]
- C2M2 (Cybersecurity Capability Maturity Model) [ ]
- CRAMM (CCTA Risk Analysis and Management Method) [ ]
- In-house developed maturity assessment framework [ ]

- If no, do you have an awareness on how your institution addresses its cybersecurity posture?

_____

_____

- How frequently does your institution conduct cybersecurity maturity assessment campaigns?
  - Annually [ ]
  - Semi-annually [ ]
  - Quarterly [ ]
- What type of assessment methodology are you using?
  - Self-assessment [ ]
  - External audit [ ]
  - Hybrid [ ]
- What areas of cybersecurity are covered in the assessment?
  - Governance and management [ ]
  - Risk management [ ]
  - Identity and access management [ ]
  - Network security [ ]
  - Cryptography [ ]
  - Operational Security [ ]
  - Incident management [ ]
  - Business continuity [ ]
  - Supply chain security [ ]
  - ATM security [ ]
  - Data Protection [ ]

- Others [ ]
- All [ ]

- If you are using in-house developed maturity assessment framework, what are the maturity levels respectively? Please tick on the box:
  - Zero (0) [ ]
  - Ad hoc (1) [ ]
  - Initial (2) [ ]
  - Defined (3) [ ]
  - Managed (4) [ ]
  - Optimized (5) [ ]
- Are there specific security standards or compliance requirements incorporated into the framework? Including national cybersecurity regulations.
  - PCI DSS [ ]
  - GDPR [ ]
  - CMCSRS (Critical Mass Cybersecurity Requirement Standard) [ ]
  - ISO27001 [ ]
  - NBE directives [ ]
  - Other, please specify _____
- How are identified cybersecurity gaps prioritized and addressed?

  _____

  _____

- How are technical professionals involved in the improvement and evolution of CMAF?

  _____

  _____

- Please share additional insights or suggestions you have regarding your institutions CMAF?

  _____

  _____

## Appendix B: Cybersecurity Maturity Assessment Framework Controls and Implementation Plan

| No. | Domain | Subdomain | Controls | Mapping the control References |
|---|---|---|---|---|
| 1 | **Cyber Governance** | Structure | Establish CS Department | COBIT 5: EDM01, CERT-RMM: Governance, ITIL: Organization Governance, CMCSRS: Governance Capability (d) |
| | | | Define Roles and responsibility | CMMI: GG2, SSE-CMM: PA02, CREST: Organizational Role Standards, CMCSRS: Governance Capability (a) |
| | | | Appoint a CISO | COBIT 5: APO01, C2M2: MIL1, ITIL: Information Security Manager Role, CMCSRS: Governance Capability (c) |
| | | | Set Annual Budget | COBIT 5: APO06, CERT-RMM: Resilience Planning, NICE CSF: OV-MGT-001, CMCSRS: Leadership Capability (j) |
| | | Guiding Frameworks | Develop CS Strategic Planning | COBIT 5: APO02, CERT-RMM: Organizational Resilience, ITIL: Service Strategy, CMCSRS: Cybersecurity Planning Process (a) (b) (c) |
| | | | Develop CS policy | HITRUST CSF: 01.b, NIST SP 800-53: PM-1, CREST: Policy guidelines, CMCSRS: Cybersecurity strategy and policy development process (a), Requirement for IT Management of Banks Directive No. SBB\|83\|2022: Article (7) 7.1 (I – XI) |
| | | | Develop CS program management | COBIT 5: APO01, SSE-CMM: PA01, FFIEC CAT: Domain 1 |
| | | | Develop CS Procedures, Processes, and guidelines | CMMI: CM, NIST SP 800-53: PM-3, ISO 27001: A.7.2, FFIEC CAT: Domain 3, CMCSRS: Cybersecurity Governance and Management process (k) (I) |
| | | Communication | CS communication channel | COBIT 5: APO07, CERT-RMM: Communication & Coordination, CREST: Communication Standard, CMCSRS: Cybersecurity |

| | | | | |
|---|---|---|---|---|
| | | | | Communication, Documentation and Knowledge Management Standard (a) (b) (c) |
| | | | Create a Reporting procedure | CMMI: GG2, CERT-RMM: Incident Management, NIST SP 800-53: PM-3 |
| | | Board Engagement | Incorporate CS into Board Setting | HITRUST CSF: 01.c, C2M2: MIL2, NIST SP 800-53: PM-3, FFIEC CAT: Board Oversight, CMCSRS: Leadership Capability (a) (b) |
| | | | Awareness for Board members | CIS Controls: Control 17, SSE-CMM: PA04, ITIL: Awareness for Senior Leadership, CMCSRS: Leadership Capability (a) |
| **2** | **Cyber Risk Management** | Risk Assessment | Develop RA methodology | COBIT 5: APO12, CMMI: RSKM, ISO 27005, FFIEC CAT: Risk Assessment, CMCSRS: Disruptive RM Process & Cybersecurity RA Process (a), Requirement for IT Management of Banks Directive No. SBB\|83\|2022: Article (6) 6.1 & 6.2 |
| | | | Conduct RA | CMMI: RSKM, NIST SP 800-53: RA-3, C2M2: MIL2, CREST: RA Standard, CMCSRS: Cybersecurity RA Process (b) (c) (d) |
| | | | Identify, Categorize, and Prioritize risks | HITRUST CSF: 03.c, CERT-RMM: Risk Management, FFIEC CAT: Risk Identification, CMCSRS: Disruptive RM Process (d) 2 |
| | | Risk Treatment | Develop mitigation strategies | CIS Controls: Control 4, COBIT 5: APO12.04, NIST SP 800-53: RA-5, ITIL: Risk Treatment, CMCSRS: Disruptive RM Process (d) 3 |
| | | | Implement mitigation strategies | CMMI: RSKM, CERT-RMM: Risk Treatment, ISO 27005, FFIEC CAT: Risk Mitigation |
| | | | Develop a risk response plan | HITRUST CSF: 03.f, CERT-RMM: Incident Management, ISO 27001: |

| | | | | |
|---|---|---|---|---|
| | | | | A.16.1, NICE CSF: Risk Response, CMCSRS: Disruptive RM Process (d) 5 |
| | | Monitoring | Develop and install a continuous monitoring plan | CIS Controls: Control 16, CERT-RMM: Monitoring & Improvement, NIST SP 800-53: CA-7, CREST: Continuous Monitoring |
| | | | Regular review of risk appetite and posture | COBIT 5: APO12, C2M2: MIL3, ISO 31000: Risk Assessment, FFIEC CAT: Domain 2 |
| | | | Conduct an audit and evaluation procedure | HITRUST CSF: 09.g, COBIT 5: MEA01, NIST SP 800-53: CA-7, CREST: Audi Guidelines |
| | | Reporting | Create a reporting line for risks managed | COBIT 5: MEA03, CMMI: PMC, CERT-RMM: Monitoring & Reporting, FFIEC CAT: Risk Reporting, CMCSRS: Cybersecurity Communication, Documentation and Knowledge Management process |
| | | | Communicate the risks to relevant stakeholders | CMMI: PMC, NIST SP 800-53: PM-3, ISO 31000, CREST: Risk Communication Standard, CMCSRS: Address Stakeholders' Security Requirements (a) (b) 3 |
| **3** | **Incident Response Plan (IRP)** | Detection | Develop and implement an Incident detection mechanism | HITRUST CSF: 11.d, CERT-RMM: Incident Management, NIST SP 800-53: IR-4, ITIL: Incident Detection, CMCSRS: Cybersecurity Incident Management Standard (a) 1 2 3 4 5 |
| | | | Deploy SIEM tools | PCI DSS: 10.6, NIST SP 800-53: SI-4, CIS Controls: Control 6, CREST: Incident Monitoring, CMCSRS: Cybersecurity Incident Management Standard (a) 3 |
| | | Response | Develop an incident response plan | COBIT 5: DSS02, CERT-RMM: Incident Management, ISO 27001: A.16, FFIEC CAT: Incident Response, CMCSRS: Cybersecurity Incident Management Standard (b) |

| | | | | |
|---|---|---|---|---|
| | | | Define roles and responsibilities in incident response | CMMI: GG2, HITRUST CSF: 11.e, SSE-CMM: PA06, CREST: Incident Role Definitions |
| | | Recovery | Develop and implement data recovery strategy | CIS Controls: Control 10, NIST SP 800-53: CP-10, COBIT 5: DSS04, ITIL: Service Recovery |
| | | | Regular update the IRP | HITRUST CSF: 11.e, CERT-RMM: Incident Management, ISO 27001: A.17, FFIEC CAT: Incident Plan Updates |
| | | Lessons Learned | Analyze post-incident status & provide a review | CMMI: MA, COBIT 5: DSS02.07, NIST SP 800-53: IR-4, CREST: Post Incident Review, CMCSRS: Cybersecurity Incident Management Standard (n) |
| | | | Archive the lessons learned from incidents | COBIT 5: DSS02.07, CERT-RMM: Monitoring & Improvement, ISO 27001: A.16.1.6, FFIEC CAT: Post Incident Analysis |
| | | | Enhance the IRP accordingly | HITRUST CSF: 11.e, CERT-RMM: Incident Management, ITIL: Continuous Service Improvement |
| **4** | **Regulatory Compliance** | Compliance Assessment | Conduct compliance assessments | COBIT 5: MEA03, CERT-RMM: Compliance Management, NIST SP 800-53: CA-2, FFIEC CAT: Compliance Management, CMCSRS: Compliance Reporting Process (a) |
| | | | Identify regulatory requirements | PCI DSS: 12.1, ISO 27001: A.18, HITRUST CSF: 13, FFIEC CAT: Domain 1, CMCSRS: Compliance Reporting Process (a) |
| | | Compliance Monitoring | Implement compliance monitoring tools | HITRUST CSF: 13.c, NIST SP 800-53: CA-7, COBIT 5: MEA03, CREST: Compliance Monitoring Tool |
| | | | Regularly audit adherence to regulations | CMMI: PI, CERT-RMM: Compliance Monitoring, ISO 27001: A.18.2.3, ITIL: Compliance Audits |
| | | Reporting | Generate compliance reports | COBIT 5: MEA03, PCI DSS: 12.9, NIST SP 800-53: CA-2, NICE CSF: OV-MGT- |

| | | | | |
|---|---|---|---|---|
| | | | | 002, CERT RMM: Compliance Reporting, CMCSRS: CMCSRS: Compliance Reporting Process (c) (d) (f) |
| | | | Report compliance status to regulatory bodies | PCI DSS: 12.8, ISO 27001: A.18.1, CERT-RMM: Reporting, FFIEC CAT: Compliance Reporting, HITRUST CSF: 13.b, CIS Controls: Control 17, CMCSRS: CMCSRS: Compliance Reporting Process (f) |
| | | Continuous Improvement | Establish processes for continuous improvement | CMMI: CAR, ISO 27001: A.18.2.3, COBIT 5: MEA01 |
| | | | Update policies as regulatory requirements change | COBIT 5: APO01.03, CERT-RMM: Policy Management, ISO 27001: A.5.1.1, CREST: Policy Evolution |
| **5** | **Mobile Money Security** | Authentication | Implement multi-factor authentication | CIS Controls: Control 6, HITRUST CSF: 12.a, NIST SP 800-53: IA-2, CMCSRS: Technology Capability (e) 6 & IoT Security Process (f) |
| | | | Use biometric authentication for transactions | HITRUST CSF: 12.a, ISO 27001: A.9.4, PCI DSS: 8.3 |
| | | Encryption | Encrypt mobile money transactions | PCI DSS: 3.1, CIS Controls: Control 13, COBIT 5: DSS05, CMCSRS: Cryptographic Management Process (a) |
| | | | Secure mobile money data in transit and at rest | COBIT 5: DSS05.05, HITRUST CSF: 06.a, ISO 27001: A.10.1.1, CMCSRS: Cloud Service Process (f) |
| | | Secure Development | Follow secure coding practices for mobile money apps | CIS Controls: Control 18, SSE-CMM: PA05, NIST SP 800-53: SA-11, CMCSRS: Cybersecurity Engineering process (a) (f) |
| | | | Regularly update mobile money platforms | COBIT 5: BAI09, CERT-RMM: Configuration Management, NIST SP 800-53: CM-2, CMCSRS: Technology Capability (g) 2 |

| | | | | |
|---|---|---|---|---|
| | | Fraud Detection | Implement fraud detection algorithms | PCI DSS: 10.2, CIS Controls: Control 6, NIST SP 800-53: SI-4 |
| | | | Monitor transactions for suspicious activities | COBIT 5: DSS05, CERT-RMM: Risk Monitoring, ISO 27001: A.10.6 |
| **6** | **Personal Data Protection** | Data Classification | Develop data classification policy | ISO 27001: A.8.2, HITRUST CSF: 09.b, NIST SP 800-53: MP-4, Personal Data Protection Regulation 1321/2024: Article |
| | | | Define access control based on the classification policy | CIS Controls: Control 6, ISO 27001: A.9.1, NIST SP 800-53: AC-3, Personal Data Protection Regulation 1321/2024: Article |
| | | Encryption | Develop encryption standard | PCI DSS: 3.1, ISO 27001: A.10.1.1, HITRUST CSF: 06, CMCSRS: Cryptography Process (a), Personal Data Protection Regulation 1321/2024: Article |
| | | | Implement the standard at data at rest and transit | PCI DSS: 3.2, COBIT 5: DSS05.06, ISO 27001: A.10.1.2, Personal Data Protection Regulation 1321/2024: Article |
| | | | Implement anonymization and pseudonymization techniques | ISO 27001: A.10.1.1, GDPR, NIST SP 800-53: SC-12, Personal Data Protection Regulation 1321/2024: Article (17) |
| | | Data Loss Prevention | Develop and deploy DLP solutions | CIS Controls: Control 13, HITRUST CSF: 09.g, NIST SP 800-53: SI-4, Personal Data Protection Regulation 1321/2024: Article (42) |
| | | | monitor and prevent unauthorize data | COBIT 5: DSS05, PCI DSS: 12.9, CERT-RMM: Data Protection |
| | | Privacy Compliance | Comply with privacy regulations | GDPR, ISO 27001: A.18, NIST SP 800-53: PT-1, CMCSRS: Information Privacy Process (a) (b) (c) (d) (e), Personal Data Protection Regulation 1321/2024: Article |
| | | | Conduct DPIA regularly | GDPR, ISO 27001: A.18, HITRUST CSF: Privacy Compliance, Personal Data Protection Regulation 1321/2024: Article (47) |

| | | | | |
|---|---|---|---|---|
| | | | Obtain necessary consent for financial and personal data | GDPR, PCI DSS: 12.8, ISO 27001: A.18, Personal Data Protection Regulation 1321/2024: Article (8) |
| **7** | **ATM Security** | Physical security | Deploy security camera | PCI DSS: 9.1, ISO 27001: A.11.1, COBIT 5: DSS05.06, CMCSRS: Physical Security Process (a) & Infrastructure Process (a) |
| | | | Install Alarm Systems | PCI DSS: 9.1, COBIT 5: DSS05, ISO 27001: A.11.1.4, CMCSRS: Physical Security Process (a) |
| | | | Install Fence | COBIT 5: DSS05, PCI DSS: 9.1, ISO 27001: A.11.1.6, CMCSRS: Physical Security Process (a) |
| | | Software Security | Regularly update ATM software | PCI DSS: 6.1, CIS Controls: Control 18, ISO 27001: A.12.6.1, CMCSRS: Technology Capability (d) 3 (f) |
| | | | Patch vulnerabilities | CIS Controls: Control 7, NIST SP 800-53: SI-2, COBIT 5: DSS05, CMCSRS: Technology Capability (d) 3 (f) |
| | | Transaction Monitoring | Install real-time monitoring system | PCI DSS: 10.6, CERT-RMM: Continuous Monitoring, COBIT 5: DSS05 |
| | | | Utilize geolocation and biometrics | PCI DSS: 9.3, ISO 27001: A.10.6.5, NIST SP 800-53: IA-5 |
| | | Access Control | Implement Multifactor Authentication | PCI DSS: 8.3, ISO 27001: A.9.4, NIST SP 800-53: IA-2, CMCSRS: Technology Capability (e) 1, 2, 3, 4, 5 |
| **8** | | Skill Development | Provide tailored CS education programs for professionals | CIS Controls: Control 17, HITRUST CSF: 01.e, COBIT 5: APO07 |
| | | | Develop technical skills through workshops and conference | COBIT 5: APO07, CERT-RMM: Workforce Development, NIST SP 800-53: AT-2 |
| | | Awareness | Develop awareness development plan | CIS Controls: Control 17, COBIT 5: APO07, ISO 27001: A.7.2.2, CMCSRS: Cybersecurity Awareness and Culture |

| | | | | |
|---|---|---|---|---|
| | **Awareness & Culture Development** | | | Development Process (a), Requirement for IT Management of Banks Directive No. SBB\|83\|2022: Article (8) 8.1 |
| | | | Conduct a regular CS awareness program | CIS Controls: Control 17, HITRUST CSF: 01.e, ISO 27001: A.7.2, CMCSRS: Cybersecurity Awareness and Culture Development Process (b) |
| | | Certification | Develop professional career path | COBIT 5: APO07, CERT-RMM: Workforce Development, CMCSRS: Human Capability (d) & Cybersecurity Awareness and Culture Development Process (d) (e) |
| | | | Certify IT/CS professionals | HITRUST CSF: 01.e, CIS Controls: Control 17, COBIT 5: APO07, CMCSRS: Human Capability (h) & Cybersecurity Awareness and Culture Development Process (a) |
| | | Talent Retention | Develop CS talent retention plan | COBIT 5: APO07, CERT-RMM: Workforce Development, NIST SP 800-53: AT-2, CMCSRS: Human Capability (h) |
| **9** | **Supply Chain Security** | Vendor Assessment | Develop vendor assessment checklist | COBIT 5: APO10, PCI DSS: 12.8, NIST SP 800-53: SA-9, CMCSRS: Supply Chain Relationship Management Process (b) |
| | | | Establish criteria for vendor selection | CMMI: SAM, PCI DSS: 12.8, HITRUST CSF: 09.g, CMCSRS: Supply Chain Relationship Management Process (b) |
| | | Contractual Agreements | Install contractual agreements in vendor contracts | PCI DSS: 12.8, COBIT 5: APO10, CERT-RMM: Supplier Agreements, CMCSRS: Supply Chain Relationship Management Process (a) (d) |
| | | | Define liability for security and privacy violations | ISO 27001: A.15.1, PCI DSS: 12.8, HITRUST CSF: 13.b, CMCSRS: Supply Chain Relationship Management Process (a) |

| | | | | |
|---|---|---|---|---|
| | | Monitoring | Implement vendor monitoring systems | CERT-RMM: Supplier Monitoring, PCI DSS: 12.8, NIST SP 800-53: SA-9, CMCSRS: Supply Chain Relationship Management Process (f) |
| | | | Register and monitor supply chain attacks | COBIT 5: DSS05, CERT-RMM: Supplier Monitoring, ISO 27001: A.15.2 |
| | | Incident Response | Define procedures for responding to supply chain activities | COBIT 5: APO10, CERT-RMM: Supplier Incident Management, PCI DSS: 12.9 |
| | | | Establish a communication channel with vendors | PCI DSS: 12.8, ISO 27001: A.15.2, COBIT 5: APO10, CMCSRS: Supply Chain Relationship Management Process (g) |
| **10** | **Network Security** | Firewall Management | Implement and configure perimeter firewalls to filter unauthorized traffic | ISO 27001: A.13.1.1, NIST SP 800-53: SC-7, COBIT 5: DSS05, CIS Controls: Control 9, CMCSRS: Technology Capability (c) 1 & 2 |
| | | | Regularly update firewall rules based on security policies | PCI DSS: 1.2.1, ISO 27001: A.12.6.1, NIST SP 800-53: SC-7, FFIEC CAT: Network Management, CMCSRS: Technology Capability (c) 3 |
| | | | Deploy Intrusion Detection and Prevention Systems (IDS/IPS) | NIST SP 800-53: SI-4, CIS Controls: Control 6, COBIT 5: DSS05, CREST: Network Security Standards, CMCSRS: Technology Capability (c) 3 |
| | | Secure Network Protocol & Cryptographic Management | Enforce secure network protocols (TLS, SSH, VPN) for sensitive data transmission | ISO 27001: A.13.2.3, PCI DSS: 4.1, NIST SP 800-53: SC-12, CIS Controls: Control 13, CREST, CMCSRS: Technology Capability (c) 6 |
| | | | Disable insecure legacy protocols (e.g., SSL, Telnet) | PCI DSS: 2.2.2, ISO 27001: A.12.6.2, NIST SP 800-53: SC-12, CIS Controls: Control 18, CMCSRS: Technology Capability (c) 6 |
| | | Cloud Security - Access Control | Implement Identity and Access Management (IAM) for cloud | ISO 27001: A.9.4, NIST SP 800-53: AC-2, COBIT 5: DSS05, CIS Controls: Control 6, CMCSRS: Cloud Service Process (a) (b) (c) |

| | | | | |
|---|---|---|---|---|
| | | | Apply Multi-Factor Authentication for cloud access | PCI DSS: 8.3, ISO 27001: A.9.4, HITRUST CSF: 12.a, CREST: IAM Standards, CMCSRS: Technology Capability (e) |
| | | | Implement tokenization for sensitive cloud data | **HITRUST CSF: 06.a**, **PCI DSS: 3.2**, **NIST SP 800-53: SC-28**, **ISO 27001: A.10.1.1** |
| | | Cloud Security – Monitoring | Deploy continuous monitoring and logging in cloud environments | **COBIT 5: DSS05, CERT-RMM: Monitoring, NIST SP 800-53: AU-2, CIS Controls: Control 6,** Cloud Service Process (c) |
| **11** | **BC and DR** | Business Continuity | Develop BC and DR plans | ISO 22301, COBIT 5: DSS04, CERT-RMM: Business Continuity, CMCSRS: Business Continuity Management Process (a) (b) |
| | | | Regularly backup critical systems | CIS Controls: Control 10, PCI DSS: 12.5, ISO 27001: A.17, CMCSRS: Backup, Recovery, and Destruction Process (a) |
| | | Infrastructure Resilience | Implement redundant systems for BC& DR | COBIT 5: DSS04, ISO 22301, CERT-RMM: Resilience Management, CMCSRS: Business Continuity Management Process (c) (d) |
| | | | Ensure data redundancy and failover mechanics | ISO 27031, COBIT 5: DSS04, CIS Controls: Control 10, CMCSRS: Backup, Recovery, and Destruction Process (e) (f), |
| | | Testing & Validation | Implement BC & DR tests/drills | ISO 22301, COBIT 5: DSS04, CERT-RMM: Continuity Testing |
| | | | Test failovers and recovery procedures | ISO 27031, CERT-RMM: Resilience Management, PCI DSS: 12.5 |
| | | Continuous Improvement | Improve BC & DR capabilities based on lesson learned | ISO 22301, COBIT 5: DSS04, CERT-RMM: Business Continuity, CMCSRS: Business Continuity Management Process (e) |
| | | | Update plans and procedures | ISO 27001: A.17.1.3, COBIT 5: DSS04, CERT-RMM: Resilience Management |

| | | | | |
|---|---|---|---|---|
| **12** | **Information Sharing & Collaboration** | Threat Intelligence Sharing | Establish policies & procedures for sharing sensitive information | COBIT 5: APO12, CERT-RMM: Threat Intelligence Sharing, NIST SP 800-150 |
| | | | Utilize automated intelligence sharing platforms | CERT-RMM: Intelligence Sharing, ISO 27010, NIST SP 800-150 |
| | | | Implement the policy through secure communication channel | COBIT 5: DSS05, ISO 27010, CERT-RMM: Incident Management |
| | | Collaboration with Regulators | Comply with applicable regulations | ISO 27001: A.18, PCI DSS: 12.9, CERT-RMM: Compliance Management |
| | | | Cross functional engagement with intelligence community | CERT-RMM: Threat Intelligence Sharing, COBIT 5: APO12, ISO 27010 |
| | | Inter-bank collaborations | Develop formal agreements between in information sharing | COBIT 5: DSS05, CERT-RMM: Threat Intelligence Sharing, ISO 27010 |
| | | | Engage in joint drill & threat analysis exercise | COBIT 5: DSS02, ISO 27010, CERT-RMM: Incident Management |
| | | | Implement NDA's or formal legal agreements | ISO 27001: A.15, PCI DSS: 12.9, COBIT 5: APO10 |
| | | Industry Forum and ISCA's | Participation in Information Sharing and Analysis Centers (ISACs) | CERT-RMM: Threat Intelligence Sharing, COBIT 5: APO12, NIST SP 800-150 |

## Appendix C: Codes and Thematic Areas

| Codes | Patterns/Sub-themes | Themes |
|---|---|---|
| - Ad hoc practices<br>- Formalized processes<br>- Incident response maturity<br>- Risk management procedures<br>- Regulatory compliance<br>- Training and awareness | - Inconsistent use of formal cybersecurity processes across banks<br>- Limited training programs for staff<br>- Partial regulatory compliance but lacking robust cybersecurity risk management strategies | *Maturity Inconsistency* |
| - ISO 27001 adoption<br>- NIST CSF integration<br>- Global best practices<br>- Third-party risks<br>- Benchmarking<br>- Cross-industry application | - International frameworks are adopted unevenly, with some banks following ISO 27001, C2M2 and NIST<br>- International frameworks like NIST CSF are perceived as more comprehensive & perfect<br>- Adoption of global best practices is limited by local resources | *Framework Applicability* |
| - Lack of integration<br>- Inconsistent implementation<br>- Mobile banking security gaps<br>- Resource limitations<br>- Vendor risk management<br>- Training deficiencies<br>- Incident response gaps | - Mobile banking platforms are under-protected<br>- Inconsistent cybersecurity implementation across departments<br>- Lack of vendor risk management processes and weak training programs | *Existing Framework deficiency* |
| - Context-specific challenges<br>- Regulatory alignment<br>- Scalability<br>- Customization<br>- Localized threats<br>- Tailored risk management<br>- Resource-efficient solutions | - Banks face unique regional threats and regulatory challenges<br>- International frameworks lack scalability and adaptability to local contexts<br>- A need for a resource-efficient, region-specific framework is identified | Necessity for Customization |

| | | |
|---|---|---|
| - Uneven policy enforcement<br>- Disparities in security measures<br>- Departmental variations in incident response<br>- Varying levels of technology use<br>- Differing adherence to protocols | - Different departments exhibit unequal application of security policies<br>- Inconsistent use of advanced cybersecurity measures across teams<br>- Incident response varies widely between operational units | *Inconsistent Security Practices* |
| - Financial constraints<br>- Limited skilled workforce<br>- High cost of technology upgrades<br>- Lack of continuous monitoring tools<br>- Insufficient budget allocation for cybersecurity | - Financial limitations hinder the implementation of advanced cybersecurity tools<br>- Shortage of skilled professionals impacts overall cybersecurity resilience<br>- Insufficient budget is allocated toward cybersecurity, slowing overall progress | *Resource Constraint* |