Addis Ababa University

Addis Ababa Institute of Technology–**AAiT**

School of Information Technology and Engineering– **SiTE**

Assessing Cybersecurity Readiness in Ethiopia Fintech Sector

By

Teklehymanot Meheret

Advisor: Elefelious Getachew (Ph.D)

Thesis Submitted In Partial Fulfillment Of The Requirements For The Degree Of Master Of Science In Cybersecurity: Cyber Governance and Management Stream

School of Information Technology and Engineering– **SiTE**

October 2024

Addis Ababa, Ethiopia

SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared by Teklehymanot Meheret entitled Assessing Cybersecurity Readiness in Ethiopia Fintech Sector and submitted in partial fulfillment of the requirement for the degree of Master of Science in Addis Ababa Institute of Technology–AAiT compiles with the regulations of the university and meets the acceptable standard the originality and quality.

Signed by Examining Board

External Examiner (Name)	**Signature**	**Date**
Internal Examiner (Name)	**Signature**	**Date**
Advisor (Name)	**Signature**	**Date**

Abstract

Ethiopian fintech sector brought a significant transformation on the financial transaction and payment instrument business. This change however poses concerns on various stakeholders that the country's ability to protect the business and to mitigate the risks caused by bad actors to exploited the vulnerability. The research aim to investigate the cybersecurity readiness and preparedness of fintech and also how their practice is met the international standard through answering three research questions.Regulators and fintech companies the major stakeholders this study utilized the proposes of got the relevant information. The research identified governance, resilience and competency as a core variable to evaluates the readiness of the sector which is very much mapped with the international standard including NIST CSF, ISO/IEC 27001 and FFIEC. The study also prepared two separates the questionnaires to address the two participants current cybersecurity practice. The collected data analyzed and observed that there is clear gap and lack of readiness. The sector lacks comprehensive framework that meet the international standard according to the research findings. There was limited practice of the backup, business continuity plan and an incident response plan which impact the resilience of the sector. The other challenge this research identified was inadequate skilled cybersecurity experts and awareness level that impacted the competency of fintech ecosystem to enhance the awareness level as well as creating cybersecurity culture. The research developed a cybersecurity assessment framework that help the sector to protect their critical assets through a proper evaluation and assessment their risk and weakness. The proposed framework subjected to went through a validation process to make sure the framework relevance to the challenged identified in the research and met the basic global standard. The research concludes with valuable recommendations and consideration to enhance cybersecurity practice, collaboration and developed tailored cybersecurity framework for continuous improvement..

Key word: *Fintech, Cybersecurity, Fintech Company, Regulator, Standard, Framework.*

Acknowledgment

First and foremost, I would like to express my deepest gratitude to God for His grace and blessings, which have guided me throughout this project and beyond. I would also like to extend my sincere appreciation and respect to my advisor, Dr. Elfilious. It has been a privilege to work under his expert guidance. His invaluable advice, support, and encouragement were instrumental in shaping this report.

I am profoundly thankful to my family for their unwavering support, wise guidance, and endless encouragement, which have been the foundation of my journey. Their love and faith in me have been instrumental in everything I have achieved. I dedicate this work to R & M, cherishing their memory always.

I am fortunate to have been surrounded by wonderful colleagues and friends who have supported me along the way, making this journey not only fulfilling but memorable. A special thank you to Musse Chekol for his significant contributions in helping me reach this milestone.

Finally, I extend my sincere appreciation to the data experts, fintech companies, banks, and institutions such as Information Network Security Administrator, National Bank of Ethiopia, Commercial Bank of Ethiopia, Ministry of Innovation and Technology, Ethio Telecom, Ahadu Bank, Buna Bank, and Safaricom Ethiopia for their invaluable insights and contributions. Their cooperation was instrumental in the success of this survey. I am also deeply grateful to the experts who dedicated their time to validate and provide valuable feedback on the proposed tools.

Acronyms

AML Anti Money Laundering. 39

C2M2 Cybersecurity Capability Maturity Model. 18

CAT Cybersecurity Assessment Tool. 16

CBE Commercial Bank of Ethiopia. 3

CIS Center for Internet Security. 18

CISO Chief Information Security Officer. 19

COBIT Control Objectives for Information and Related Technology. 21

CSF Cyber Security Framework. 7, 17

ECA Ethiopian Telecommunication Authority. 10

FFIEC Federal Financial Institutions Examination Council. 16

INSA Information Network Security Administrator. 3, 9

ISC² International Information System Security Certification Consortium. 21

ISO International Standard Organization. 17

KYC Know Your Customer. 39

MiNT Ministry of Innovation and Technology. 3

NBE National Bank of Ethiopia. 3, 9

NCSC National Cybersecurity Center. 16

NIST National Institute of Standards and Technology. 17

USD United States Dollar. 9

Glossary

CFC CFC represents the independent variable that evaluates the competency of personnel in managing and executing cybersecurity strategies within fintech Companies, focusing on their skills, knowledge, and expertise in safeguarding digital assets. 31

CFR CFR represents the independent variable that evaluates the competency of personnel in managing and executing cybersecurity strategies within regulatory bodies, focusing on their skills, knowledge, and expertise in safeguarding digital assets. 29

GFC GFC represents the independent variable used to assess the effectiveness of governance frameworks in overseeing and implementing cybersecurity practices within the fintech companies.. 31

GFR GFR represents the independent variable used to assess the effectiveness of governance frameworks in overseeing and implementing cybersecurity practices within the regulatory bodies.. 29

PFC PFR is the dependent variable used to measure the overall cybersecurity readiness of the fintech for fintech company. It reflects how well the sector is equipped to protect its critical digital assets and infrastructure from cyber threats, taking into account various influencing factors such as governance, resilience, and competency.. 31

PFR PFR is the dependent variable used to measure the overall cybersecurity readiness of the fintech sector in Ethiopia. It reflects how well the sector is equipped to protect its critical digital assets and infrastructure from cyber threats, taking into account various influencing factors such as governance, resilience, and competency.. 29

RFC RFC refers to the independent variable used to evaluate the resilience of regulatory bodies in maintaining and enforcing cybersecurity measures within the fintech companies.. 31

RFR RFR refers to the independent variable used to evaluate the resilience of regulatory bodies in maintaining and enforcing cybersecurity measures within the regulatory bodies.. 29

List of Figures

List of Tables

Contents

1 Introduction

1.1 Background Information

The rapid evolution of digital technology had led to profound changes in various facets of human life, significantly enhancing connectivity, financial inclusion, and access to trade, markets, public services, and technological advancements. Developing countries, in particular, have witnessed the transformative potential of digital technology, which has reshaped entire industries and sectors[1]. One of the most notable developments within this digital revolution is the rise of the financial technology (fintech) industry, which refers to the application of technological innovations to deliver financial services and solutions. Fintech encompasses a diverse array of businesses, funding mechanisms, and geographical contexts, making a substantial impact on the global financial sector [2]

The emergence of fintech as a vital component of digital business environments highlights the need for adherence to international standards and compliance with regulations. This study recognizes the significance of cybersecurity policy to manage the entire process of financial transactions conducted using technology. Compliance with controls and regulations is not only necessary but also mandatory to ensure the convenience, safety, and resilience of the fintech ecosystem[54].

As characterized in the literature, the fintech sector is distinguished by a suite of interconnected financial technologies, driven by a culture of innovation and data-centric operations. This industry represents a rapidly expanding domain that integrates elements of traditional banking with modern financial services, challenger banks, and an array of start-ups. The sector's progressive nature is evident in the wide range of services it offers, including payments, alternative finance, mobile retail banking, currency exchange services, investment platforms, and the integration of cryptocurrencies[3].

Fintech enterprises are transforming the traditional financial system by extending their reach to underserved populations, particularly non-banking individuals in rural areas[4]. This expansion has the potential to significantly alter the landscape of business transactions and financial services. The advent of digital technology has opened up new opportunities within the financial sector, allowing new entrants to introduce innovative services and products. Companies and start-ups trying to take their share, leveraging the technology offering financial services and products.[5].

However this sector highly targeted by cybercriminal and attacker that makes proportionally vulnerable for cyberattack and threat actors that leads to experienced huge financial losses, with firms in this industry being 300 times more likely to experience such incidents compared to other sectors[8]. The fintech industry, as a crucial component of the global financial ecosystem, faces big threats. Projections indicate that the global costs of cybercrime are expected to rise by 15 percent annually, potentially reaching an alarming United States Dollar 10.5 trillion per year by 2025[9].

Fintech companies are known by their flexibility, adopt technology, and take calculative risks. It is important to acknowledge such behavior to continues reshape banking practices, incorporates new features in areas like payments, insurance, remittances, lending, and wealth management. yet, it requires to recognize that the attractiveness and targeted nature of fintech also present complex and dynamic cybersecurity challenges that must be dealt carefully [17].

In Africa, the average cost of a cybersecurity breach is estimated at $3.86 million, surpassing the global average of $3.62 million. The rapid digitization of business operations, particularly within the financial sector in Sub-Saharan Africa, offers substantial economic opportunities, including job creation and the emergence of new businesses. However, this rapid digital transformation also introduces brought cybersecurity threats. The continent is estimated to incur economic losses of approximately $4 billion annually due to cybercrime, with South Africa, Nigeria, and Kenya bearing the brunt of these losses, estimated $570 million, $500 million, and $36 million per year, respectively[10].

In the context of Ethiopia, it is difficult to get the correct data in this regard but compared to other African countries the industry in its infant stages, despites there is a rapid growth and initiatives. Both the Ethiopian government and private sector are playing active roles in advancing the fintech ecosystem. Regulatory bodies such as the National Bank of Ethiopia National Bank of Ethiopia, the Information Network Security Agency Information Network Security Administrator, and the Ethiopian

Communications Authority Ethiopian Telecommunication Authority are introducing new legislations and policies to create a conducive business environment for fintech companies[6].
On the other hand, private companies increasingly adopting fintech solutions, integrating new payment options to complement traditional transactions, enhance customer experience, and expand their customer base. The adoption of digital technology in the financial sector presents opportunities for seamless financial transactions, enabling users to make convenient payments via mobile devices, regardless of geographical location[6]. This digital transformation in financial services holds the potential to drive economic growth, promote financial inclusion, and empower individuals and businesses across the country. However, alongside these opportunities, the sector always at risk from cybersecurity threats.
Key financial market infrastructures, such as payment and settlement systems, trading platforms, central securities depositories, and central counterparties, are identified as critical components whose compromise could result in severe financial disruption . The significance of these infrastructures as potential single points of failure emphasizes the need for heightened cybersecurity vigilance [11].

Given the evolving nature of Ethiopia's fintech industry and the associated cybersecurity risks, it is imperative to assess the security readiness of fintech companies and regulatory bodies. On the other hand, the government's ability to safeguard citizens from cyber-attacks and financial fraud remains a big worry. Various stakeholders, including cybersecurity experts and IT professionals, have reflect concerns regarding these issues[13].

In order to fill the existing information gap and develop a clearer picture of the cybersecurity obstacles encountered by Ethiopia's fintech sector, this study endeavors to offer valuable perspectives for policymakers, researchers, industry professionals, and technology users. Through a detail examination, the research assess the security readiness of the fintech industry, ultimately aiding in the growth and resilience of Ethiopia's fintech environment.

The attack surfaces within the financial sector have expanded dramatically due to the digitization of financial services and the shift to remote work[12]. This increased vulnerability has been accompanied by a rise in the intensity and sophistication of cyberattacks, necessitating strong interventions through research and development, as well as the formulation of stringent cybersecurity policies, particularly within the financial sector.

By identifying gaps and proposing necessary measures, this research offer frameworks, standards, guidelines, procedures and tool tailored to the unique needs of the fintech industry. Ultimately, this study seeks to enhance the industry's ability to protect users, companies, and the nation from cybersecurity threats.

1.2 Statement Of The Problem

In Ethiopia, the financial technology (fintech) landscape has undergone a significant transformation due to the swift policy changes by the government, aimed at leveraging technology to enhance financial inclusion for citizens and to attract a diverse range of businesses. This progress has been facilitated through collaborative efforts among regulatory bodies, businesses, technology startups, and telecommunication companies, leading to substantial advancements in technology adoption. These stakeholders have played a crucial role in the development of the financial sector by implementing new regulations, embracing innovative technologies, and forming strategic partnerships to attract fintech enterprises and businesses [52]. While these developments hold promise, concerns have surfaced regarding the country's readiness to securely manage technology-driven financial transactions, especially considering its current level of digital proficiency and security awareness.

Furthermore, the lack of detailed strategies, frameworks, standards, and technologies customized to meet the specific requirements of Ethiopia's fintech industry intensifies these worries. This deficiency in cybersecurity readiness not only jeopardizes the security of crucial financial assets but also poses a threat to the overall resilience of the fintech supply chain. Therefore, it is crucial to conduct a comprehensive evaluation of the cybersecurity readiness of organizations and businesses in the Ethiopian fintech sector. Such an evaluation is vital for identifying vulnerabilities and establishing a secure and robust fintech environment capable of efficiently countering cyber risks[51].

1.3 Research Questions

The fintech industry has swiftly become a significant player in Ethiopia's business realm, despite its recent inception. Although government efforts have nurtured its development through diverse interventions, uncertainties persist regarding the nation's readiness to fully integrate fintech solutions. This thesis aims to explore the existing cybersecurity protocols in Ethiopia's fintech sector, pinpoint crucial deficiencies, and assess the industry's overall cybersecurity readiness. To measure this readiness, the research aims to address the following key questions:

- What are the cybersecurity practices employed by fintech companies in Ethiopia?
- What are the critical gaps in cybersecurity readiness within Ethiopia's fintech sector?
- What practical cybersecurity assessment framework can be proposed to improve cybersecurity readiness?

The study aims to provide valuable insights on cybersecurity practices by fintech sector in Ethiopia through these research questions. It identify areas requiring improvement and offer practical recommendations to enhance cybersecurity readiness within the sector. Ultimately, the findings of this research contribute to the development of a strong cybersecurity environment, promoting resilience in Ethiopia's fintech industry.

1.4 Objective Of The Thesis Study

1.4.1 General Objective

The main objective of this research to assess cybersecurity readiness of Ethiopian's fintech sector current practice, identify gaps and propose assessment framework.

1.4.2 Specific Objective

The specific objectives of the study:

- To asses existing cybersecurity practices by fintech sector;
- To identify key challenges and gaps in cybersecurity practice;
- To propose cybersecurity assessment framework.

1.5 Contribution Of The Thesis Study

The major objective of this thesis to the Ethiopian fintech ecosystem cybersecurity readiness by conducting a comprehensive assessment to identify the major challenges companies facing, their gap in current practice and developed assessment framework.

This research project contributes the countries cybersecurity ecosystem as an input particularly for fintech to developed an assessment framework for the industry to address the pressing issue of their business process by laying the foundational data about their practice so that to introduce the right solution to mitigate risks and minimize their potential effects on the fintech ecosystem. The research involved major players in the industry, including regulatory bodies and fintech companies, offering a broad analysis of cybersecurity practices. The researches finding reflects overall cybersecurity practice of the country and companies' readiness by identifying gaps, challenges and major security requirements to mitigates risks. .

From policy perspective, this research provides valuable insights for policymakers and legislators, to use this research finding as a reference to develop regulation and legislation to address critical gaps identified during this assessment.

Since there is a limitation of research in these areas, the thesis adds an existing knowledge gap by providing new insights and real-world data. It serves as a valuable foundation for future research focused on improving cybersecurity practices and reducing the risks of security breaches and technology misuse.

Finally, the proposed assessment tool offers a practical resource for fintech companies, banks, regulators, start-ups, and consultants. Using the proposed framework, organizations able to know their gaps and invest on the right solution which increased investor and user confidence for the industry to anticipate the cybersecurity practice and culture. It helps companies evaluate their cybersecurity stance and educates employees on the importance of security and its consequences. This tool strengthens the industry's ability to handle security incidents and improves overall cybersecurity resilience across the ecosystem.

1.6 Scope

The purpose of this research is to find out the cybersecurity readiness of the Ethiopian fintech industry, with a particular emphasis on areas that may reveal significant gaps and challenges in the industry and develop an assessment framework. The study's participants can be divided into two main groups: fintech startups and regulatory agencies. In order to address the nation's cybersecurity preparedness and practice, the study attempts to provide answers to three research questions. Therefore, the study examines current practices, finds gaps, and suggests a workable framework that improves cybersecurity practices in the industry while adhering to global norms.

2 Literature Review and Related Works

This section explored various research papers, articles, and publications within the fintech industry, focusing particularly on cybersecurity and related research topics to grasp global trends.

In essence, through an analysis of previous works, this section aimed to identify existing gaps that require attention, especially concerning Ethiopia's unique circumstances. This contextual understanding played a crucial role in shaping the tangible outcomes and contributions of the completed thesis project.

2.1 Introduction

Fintech has dynamically changed the financial industry by revolutionizing banking, payments, asset management, and insurance. According to [18], fintech transform the way how transactions are conducted by disrupting conventional banking practices and financial ecosystems. The widespread use of mobile technology and smart devices has improved financial inclusion while also making financial services more convenient and effective.

But these technologies' quick adoption has also brought up new cybersecurity difficulties. According to this paper[19], tackling cybersecurity risks is essential for the long-term viability of fintech due to the growing dependence on the internet and mobile devices.

According to research given at an international conference in 2021, privacy and security issues are major obstacles in fintech's data consumption, but the integration of technology into finance has also resulted in tremendous value development for businesses [13]. Fragmented banking rules are another issue highlighted in the World Economic Forum's 2020 Cyber Resilience Report, which makes it challenging to create safe cross-border fintech solutions[4].

Global trends indicate that cybersecurity frameworks and capacity-building programs within fintech companies, particularly in developing nations, must advance along with technology. The increasing dependence on third-party providers and networked services makes financial market infrastructures more susceptible to hackers, claims [76]. Therefore, protecting sensitive financial data and guaranteeing long-term viability in the fintech ecosystem require a proactive approach to capacity building and keeping current cybersecurity knowledge.

According to the ITU's Global Cybersecurity Index (2020), many poor nations' inability to employ enough cybersecurity experts has a direct effect on their capacity to manage advanced cyberthreats. Additionally, it is anticipated that by 2025, there will be a skills gap in cybersecurity of over 3 million people worldwide, with developing countries being the most affected because they have less access to training and educational materials.[75]

2.1.1 Cybersecurity in Developing Countries

The least developed nations' poor infrastructure, lack of appropriates regulations, and low level of cybersecurity awareness make the industry highly prone to cyber threats. The 2020 World Bank research emphasizes how fintech companies are vulnerable to cybercrime due to disjointed cybersecurity laws and lax enforcement. Similar to this, [19] highlights how fraudsters operate globally and how difficult it is to secure interconnected financial networks, which makes these vulnerabilities worse.

Inadequate skilled workforce capable enough anticipate, managing, and reducing cybersecurity threats. According to a 2019 International Telecommunications Union (ITU) report, many developing countries struggle with a lack of human capital, which makes it difficult to implement cybersecurity frameworks that work [19]. This forces local fintech firms to rely on foreign consultants and third-party services, which aren't always available or economically viable.

For Ethiopia, digital transformation is seen as a driving force for economic reform across sectors like agriculture and manufacturing, as outlined in the country's 2020 National Digital Strategy [22]. However, cybersecurity readiness remains a significant barrier. [21] argues that identifying digital infrastructure requirements and integrating third-party services while minimizing cybersecurity risks are essential steps to ensuring smooth and secure fintech operations. Ensuring data privacy, particularly in international

13 transactions, is also vital, with compliance to the General Data Protection Regulation (GDPR) being a critical aspect [13].

2.1.2 Role of Regulatory Bodies

The development of cybersecurity guidelines for the fintech sector is heavily influenced by regulatory agencies. Regulatory frameworks can require strict data protection procedures, incident reporting, and multi-factor authentication, as demonstrated by the European Union's General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2) (World Bank, 2020). However, similar standards are not being adopted as quickly in underdeveloped nations like Ethiopia, which makes the sector more vulnerable to cyber threats.

This research paper, [64] highlights the complexities of regulating the interconnected and increasingly sophisticated financial systems. In Ethiopia, regulators have started recognizing the importance of cybersecurity, but gaps in policies still pose a threat to fintech growth.[69] suggests that adopting global best practices, such as those embedded in GDPR, would help Ethiopia bolster its fintech sector's resilience against cyber threats.

The Financial Stability Board's (FSB) 2017 report [72] emphasizes the dangers of disjointed cybersecurity regulations, especially for international digital financial services. The FSB notes that managing cyber risks in the fintech industry is more difficult due to the absence of uniform norms across jurisdictions. Given the interconnectedness of fintech operations, the research emphasizes the necessity of international regulatory organizations cooperating to provide a more coherent and uniform global framework.

In addition, the 2021 IMF Working Paper [73] examines the necessity for regulators in emerging markets—particularly in Africa—to cooperate with global organizations and take adaptable measures in order to guarantee the safe expansion of regional fintech ecosystems. The study emphasizes how access to global cybersecurity resources and knowledge may be made possible through international cooperation, which can also assist close gaps in local expertise.

2.1.3 Financial and Economic Impact of Cybersecurity Breaches

Cybersecurity breaches can have significant financial and economic effects for fintech companies. The average cost of a data breach in fintech organizations, including direct and indirect costs, is about $1.52 million, per an IBM Security survey [35]. Such breaches usually result in a loss of consumer trust, legal implications, and damage to one's reputation. Furthermore, 80% of consumers are likely to give up doing business with a company after a data breach, which causes a significant loss of revenue, according to IDC.

Additionally, due cyberattacks have a cumulative impact on interrelated companies within the finance industry, they may hamper service delivery throughout supply chains. A notable case is the June 2017 ransomware attack on Ukraine, which cost multinational companies connected to Ukrainian enterprises in a range of sectors, including food and transportation, over $1.3 billion in losses [36]. The risks are exacerbated by the fact that fraud and data breaches account for 43% of major cyber occurrences in the financial industry. Cyber threats are more challenging to identify because of their dynamic nature, which could lead to long-term financial loss [36].

Accenture estimates that over the next five years, cybercrime could cost big corporations up to $5.2 trillion in losses. This study draws attention to the growing financial dangers, especially in high-tech sectors where billions of dollars are at risk. The issue is made worse by the growing dependence on internet-based business models, which is outpacing the creation of adequate cybersecurity protections. Cyberattacks put businesses at risk for innovation and growth in addition to immediate financial losses [70] [71][70] [71].

In conclusion, cybersecurity breaches in fintech can lead to direct financial losses, disruption of services, loss of intellectual property, and reputational damage [37]. As fintech continues to grow, particularly in developing regions like Ethiopia, the importance of strengthening cybersecurity measures cannot be overstated.

2.2 Related Works

Fintech, an abbreviation of financial technology, represents an innovative approach that creates services aiming to compete with traditional offerings[19]. One research paper analyses the effects of cybersecurity variables on fintech, using self-efficacy (SE), information security experiment (IS), technology culture (TC), competence and skill (CS) as independent variables, and cybersecurity as the dependent variable. The study proposes a model to examine their relationship and finds a highly positive correlation between fintech and cybersecurity, suggesting that a one-unit increase in fintech corresponds to an increase in cybersecurity[19]. While this study examines the relationship between cybersecurity and fintech using four specific variables, it does not consider other factors such as regulations, compliance, standards, and procedures that significantly influence fintech security. Thus, the assessment proposed in this study aims to fill this gap.

Another research paper investigates the adoption of financial technology among Ethiopian banking customers. The study finds that adoption is influenced by customer awareness, subjective norms, and perceived usefulness. Its further highlights that in countries like Ethiopia, where social collaboration is high, the perception of friends, colleagues, or family members plays an important role in influencing adoption motivation. However, the paper does not specifically address the effects of security on the technology adoption process and government rule and regulation, beyond the factors mentioned. In this context, security plays a crucial role in the adoption of any technology, particularly in the financial space[24]. The literature review reveals that a lack of comprehensive studies on cybersecurity readiness at the national and organizational levels, as identified in some of the reviewed papers. This serves as motivation to conduct assessments within the fintech ecosystem, focusing on Ethiopia.

2.2.1 Cybersecurity Practice In Fintech Ecosystem

FinTech companies in developing countries such as Ethiopia face several challenges regarding cybersecurity readiness. According to [25]cybersecurity is the top challenge and a major legislative concern for FinTech business.

A World Bank study identified that cybersecurity in developing countries faces challenges in adjusting fintech companies' perspectives on policy, processes, and required behaviors, which highly increase the industry's risk of cybercrime and technological failure [26].

An article published on [27] highlighted the importance of collaboration all stakeholders engaged in the Fintech industry established a forum to tackle the cybersecurity by enabling a collaboration platform, developing common standards and create a communication channel as well as information exchange platform. The paper also emphasizes the importance of multi-stakeholder approach to going forward to address cyber related crimes in developing countries.

A research paper identified that cybercriminals are not only targeting consumers and service providers, regulatory bodies who are handling confidential and sensitive information in the financial sectors. One classical example according to this research is an incident happened in 2016 at Bangladesh's central bank cyber heist by installing a malware on the IT system and managed to stole USD 81 million[28].

2.2.2 Major Cybersecurity Readiness Gaps In Fintech Industry In Developing Nations?

One of the biggest gaps that is practically existed in developing countries to build resilient ecosystem is lack of a strong regulatory framework that can protects ordinary citizens from any mischiefs and fraudulent[26]. Financial institution losing millions of dollars every year due breaches and criminal activity. A study covering over 700 organizations in Africa revealed that the banking sector suffered a USD 1.05 trillion loss due to cyberattacks in 2017[26].

According to [29] despite the current lack of well established regulatory ecosystem, the proliferation of diverse fintech solutions has prompted regulators to expand their focus. Notably, 2021 witnessed the introduction of regulatory frameworks targeting previously unregulated sectors like equity crowdfunding and open banking. Nevertheless, the literature underscores the persistent issue of sudden regulatory shifts, exemplified by the Central Bank of Nigeria's ban on crypto assets, which continues to pose major

obstacle to the stability and growth of Nigerian fintech enterprises.

User trust is one of the essential components to materialize the fintech cybersecurity readiness for the ecosystem. Individuals or organization relied on the technology to deal business transaction and the two party who are involved should trust the system and the governments responsible to facilitate the trusty through various interventions including building digital infrastructures that are important to protect and guaranty the players from any malicious activity in the ecosystems. Despite the importance of cybersecurity in build trust in the digital realm, it has been neglected in many parts of the world. While some countries have enacted cybersecurity laws and regulations, others lack adequate measures or have none at all[30].

Skilled man power in the area of cybersecurity in particular developing countries like Ethiopia faced a huge challenge to find the right person which widen the vulnerability of the industry and unable to deploy proactive measures to minimize risks and anticipate threats landscape to protect critical assets. According to [33] stated that in Kenyan companies encounter difficulties in recruiting cybersecurity experts. When asked about the obstacles they encounter during the hiring process, managers commonly point out two primary challenges: a shortage of experienced candidates and the high salary expectations of potential hires.

In the realm of cybersecurity readiness, the literature underscores the growing importance of addressing operational risks, which encompass cyber threats, fraud, and internal errors, especially in the context of the digital age[34].

2.3 Review Existing Cybersecurity Readiness Assessment Standard, Framework and Tools

There are well-defined and comprehensive cybersecurity frameworks currently in existence, adopted for various use cases. These frameworks and standards provide a solid foundation for developing a tailored cybersecurity readiness assessment tool specifically for the fintech sector in Ethiopia. While these frameworks are detailed and extensive, they are designed to be adapted to specific contexts to fully realize their potential. By understanding the framework, it can be created a customized tool that enhances organizational capabilities a situation where there is a resource limitation, lack of skilled experts and ad-hoc process to practice the cybersecurity practice.

2.3.1 FFIEC Cybersecurity Assessment Tool (CAT)

The Cybersecurity Assessment ToolCybersecurity Assessment Tool from the Federal Financial Institutions Examination Council One methodology created by the Federal Financial Institutions Examination Council in the United States that used as a cybersecurity assessment tool for financial institutions and organizations to evaluate their cybersecurity readiness and find identify vulnerability and weakness.

The tools main purpose is design measurable and reputable process to assess institution's level of cybersecurity risk and preparedness. The tools has two main parts to assess company's readiness. The first part is inherited risk profile related to cyber risk and the second part is Cybersecurity Maturity, which determines an institution's current state of cybersecurity preparedness represented by maturity levels across five domains[40].

This tools can be adopted and used to a similar scenarios and organization who are mainly engaged in financial business. There are wide areas that are covered in the frameworks through different aspects of cybersecurity and this research could emulates requirements for the countries fintech space challenges identified in this study result.

2.3.2 NCSC CAF Cyber Assessment Framework

The NCSC Cyber Assessment frameworkNational Cybersecurity Center was created by the UK's National Cyber Security CentreNational Cybersecurity Center to assist companies in evaluating their cybersecurity posture and identifying areas that need improvement. The procedure can be used to evaluate a nation's overall cybersecurity readiness, even though its primary purpose is for corporations [41].

The CAF is organized around four fundamental tenets, according to [41]: controlling security risk, preventing cyberattacks, identifying cyber security events, and lessening the effects of cyber security disasters.

The cybersecurity assessment framework support organization to responsible for vitally important services and activities. The framework is designed to be utilized in combination with existing cybersecurity standards and frameworks, such ISO 27001 or NIST [42].

2.3.3 CIS Critical Security Controls

An established procedure known as a CIS critical security control is used by the Center for Internet Security to help organizations identify and rank their most important cybersecurity needs. The controls were initially created to help small businesses strengthen their cybersecurity defenses, but they may be used for any reason to gauge a country's or region's cybersecurity posture and readiness.

The center identified 18 best practices for cybersecurity control in order organization to prioritized their important process and resources to protect sensitive information and assets depending on their business needs and objectives. The controls organized in three categories:

- Basic
- Foundational
- Organizational

A key benefit of CIS Controls is the focus on actionable, results-driven measures that can be implemented quickly and effectively[42].

2.3.4 NIST Cybersecurity Framework Cyber Security Framework

The National Institute of Technology National Institute of Standards and Technology Cybersecurity Framework, which offers a comprehensive and adaptable approach to mitigating cybersecurity risks. The framework can be modified and used to solve the specific cybersecurity issues faced by fintech businesses operating in Ethiopia, even though it is not especially designed for the fintech industry [43].

When measuring cybersecurity readiness of Ethiopian fintech ecosystem, the NIST Cybersecurity Framework can be highly useful. Fintech companies may efficiently assess current state of cybersecurity and highlight opportunities for development by implementing the framework's standardized process.

The framework includes an in-depth structure to assess numerous aspects of cybersecurity readiness thanks to its main roles of Identify, Protect, Detect, Respond, and Recover. The Identify function, for example, helps fintech organizations to understand the potential cybersecurity risks and threats they are face and create inventory for critical assets, systems, and data. While the Detect function facilitates in the deployment of optimal monitoring and detection systems, on the hand Protect function directs businesses in establishing proper protections mechanism to mitigates risks. The Respond and Recover functionalities guarantee that fintech companies developed a business continuity plans and incident response plans efficiently handle and recover from security breaches[44].

Fintech organizations can also prioritize their cybersecurity efforts according to their unique risk profiles thanks to the NIST Framework's risk-based approach. Fintech companies can efficiently allocate resources and concentrate on areas that pose the greatest threats to their operations and customers by conducting in-depth risk assessments and aligning their cybersecurity measures with the risks that have been identified. In the fast-changing fintech industry, where new services and technology are constantly being introduced and could bring new cybersecurity challenges, this risk-based approach is particularly important.

2.3.5 ISO 27001

The widely accepted and widely used International Standard Organization(ISO) 27001 framework is used by many organizations to establish an information security management system (ISMS), which helps businesses adopt, maintain, and enhance cybersecurity practices. By assessing important sectors

and infrastructure through the implementation of ISMS principles and control, the framework may be adopted and utilized to measure for national cybersecurity readiness and preparedness.

Fintech businesses can safeguard their data from numerous threats by complying to these recommendations, guaranteeing that it is private, undamaged, and only available to authorized users [[45]. Building evaluation instruments to pinpoint and resolve their unique security flaws and restrictions is another aspect of this.

2.3.6 Cybersecurity Capability Maturity Model (C2M2)

Cybersecurity Capability Maturity Model (C2M2) well known framework for investigation organization maturity in their cybersecurity practice and culture. This procedure aids organizations in planning to correct their posture in a systematic and controlled manner. This kind of action is a sign that businesses are strategically aligning themselves with globally recognized practices in order to accomplish their commercial objectives. The framework included a structure that aids organizations and security actioners in conducting cybersecurity assessments in order to find out vulnerabilities. This approach is especially beneficial as the fintech industry places a high priority on the security of financial data and systems [46].

Fintech companies can quickly adopt and implement the framework to reduce ecosystem risk in their daily transactions, which are highly vulnerable to attacks and breaches by a variety of actors. To protect and fully understand their capabilities against international standards and industry best practices, Cybersecurity Capability Maturity Model (C2M2) might be quite important

2.3.7 CIS Controls

A set of priority measures aimed at reducing the most frequent cyberattacks is known as the Center for Internet Security Controls. As the fintech sector deals with extremely sensitive financial data, Center for Internet Security (CIS) Controls implementation offers a useful and efficient way to improve cybersecurity preparedness. Through adherence to these policies, fintech organizations can handle important aspects of cyber hygiene, including safe hardware and software configuration, ongoing vulnerability management, and inventory and control of hardware and software assets. Because of its three Implementation Groups (IG1, IG2, and IG3), the framework is especially well-suited for fintech enterprises with different levels of cybersecurity maturity and resources. This allows organizations to prioritize actions according to their risk profiles and available resources.

Implementing CIS Controls helps fintech companies create a cybersecurity foundation by focusing on essential and prioritized actions. For instance, starting with IG1 ensures that basic cyber hygiene practices are in place, providing immediate security improvements without requiring extensive resources. As fintech companies progress to IG2 and IG3, they can build on this foundation by implementing more advanced controls, such as incident response and management, penetration testing, and application software security. This structured approach enables fintech companies to incrementally enhance their cybersecurity posture, ensuring that they can protect sensitive financial information, comply with regulatory requirements, and maintain customer trust[47].

3 Research Methodology

3.1 Introduction

This section outlined the research methodology employed in this study. It refers to the systematic approach, methods, and procedures used to investigate specific research questions scientifically. The methodology ensures that the research outcomes are reliable, valid, and replicable. The section covers the research design, data collection methods, sample size determination, validation techniques, research variables, the research model, and analysis procedures.

By providing a detailed explanation of the methodology, this section offers insights into how the research was conducted and the steps taken to derive meaningful and credible results.

3.2 Research Design

This study employed a descriptive research design, adopting a quantitative approach to investigate the cybersecurity readiness of Ethiopian fintech companies. By focusing on quantifiable data, the research systematically addressed the technological and organizational factors that influence cybersecurity readiness within the sector. The design allowed for a thorough analysis of measurable variables, ensuring an objective evaluation of the state of cybersecurity.

3.2.1 Source Of Data

The primary data was gathered through structured surveys using a detailed questionnaire. The survey was carefully designed to understand key areas of cybersecurity readiness, focusing on governance, resilience, skills, and preparation. Each survey question used Likert scales, allowing respondents to indicate how much they agreed or disagreed. This allowed for a detailed analysis of the cybersecurity practices and policies used by Ethiopian fintech companies.

The participants in this study were identified based on their roles within the fintech industry. This involved visiting their companies and speaking directly with people in roles like Chief Information Security Officer Chief Information Security Officer or cybersecurity manager, who are responsible for managing cybersecurity in their respective institution.

3.2.2 Variables

The study analyzed four dependent variables and one independent variable, selected for their relevance to the Ethiopian fintech industry and their role in digital financial services. These variables played a critical role in assessing the cybersecurity readiness of both fintech companies and regulatory bodies. By focusing on these variables, the research was able to capture key factors influencing the cybersecurity landscape.

To determine the appropriate variables for this study, the Technology-Organization-Environment (TOE) framework, originally proposed by Tornatzky and Fleischer (1990), served as the foundational model for identifying key factors influencing cybersecurity readiness within the Ethiopian fintech sector. The TOE framework offers a holistic perspective to analyze the interplay between technological factors, organizational characteristics, and environmental influences [31]. Leveraging this framework, Governance, Resilience, and Competency were identified as critical dependent variables to assess cybersecurity readiness.

The TOE framework has been widely adopted in various contexts, including the adoption of technological innovations [55] and information systems research [56]. Its applicability to cybersecurity domains has also been recognized [57], as it provides a comprehensive lens to examine the multifaceted factors influencing cybersecurity preparedness.

By utilizing the TOE framework as a guiding theoretical model and connecting the study's key variables – Governance, Resilience, and Competency – with its corresponding technological, organizational, and environmental aspects, a strong theoretical basis is formed. This approach facilitates a systematic analysis of the complex relationships among these crucial factors, clarify their combined impact on determining

cybersecurity preparedness within the ever-evolving Ethiopian fintech sector.

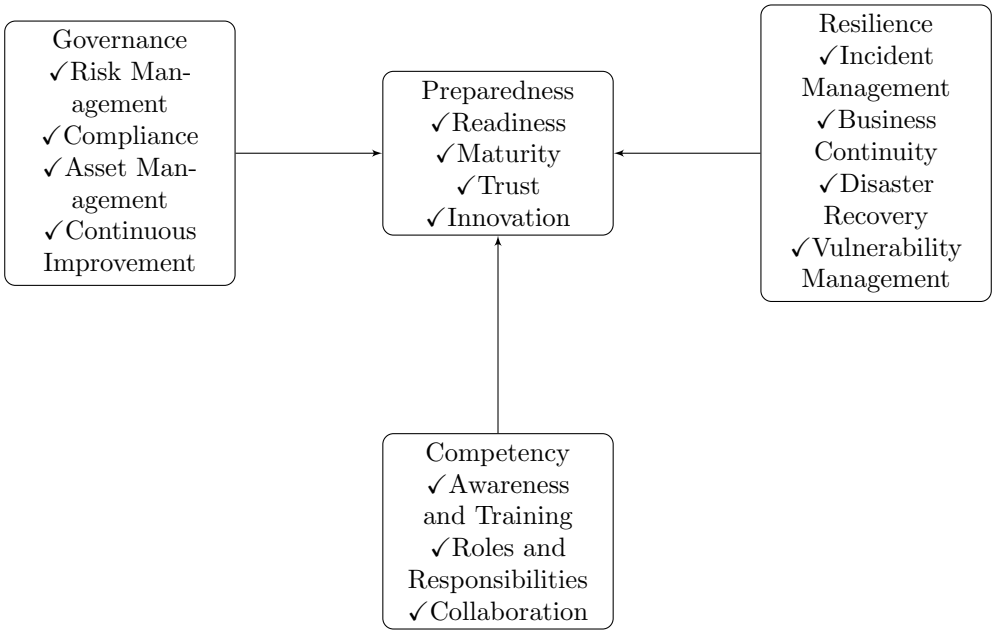


Figure 1: Variable Relationship

Meaning and Definitions of Variables Used In The Study

1. **Independent Variables**

   (a) **Governance**
   In the context of organizations, governance refers to the rules, procedures, legal frameworks, governance structures, enforcement framework, and compliance procedures that direct accountability, supervision, and decision-making. Governance was essential to bolstering an organization's security posture in terms of cybersecurity readiness. Organizational traits including management support, organizational structure, and resource allocation are important elements influencing technology adoption, according to the Technology-Organization-Environment (TOE) framework [58].

   In this study, effective governance ensured that cybersecurity strategies aligned with organizational objectives, risk tolerance, and regulatory requirements. It also facilitated the allocation of necessary resources, including budget, personnel, and infrastructure, to implement and maintain cybersecurity measures. Governance further included asset management practices, such as identifying, classifying, and protecting critical information assets. By incorporating governance as a variable, the study assessed how organizational factors—such as leadership commitment, decision-making processes, and policy frameworks—impacted cybersecurity preparedness in Ethiopia's fintech sector.

   Theoretical Basis:

   - The NIST Framework for Cybersecurity (CSF): The NIST CSF's "Identify" function highlights how crucial governance is to comprehending and controlling cybersecurity threats.Companies with a mature cybersecurity posture must have a defined framework for decision-making, accountability, and policy-setting, which governance guarantees.

   - The creation of an information security management system (ISMS) is the main objective of ISO/IEC 27001. This standard emphasizes the importance of governance in controlling information security risks through rules, regulations, and controls.

- Practical Frameworks: Governance is a cornerstone in frameworks like Control Objectives for Information and Related Technology 5, which provides a comprehensive approach to IT governance and management, ensuring that cybersecurity efforts align with overall business goals.

(b) **Resilience**
The ability of an organization to tolerate, adjust to, and recover back from cybersecurity events or interruptions was referred to as resilience. It included putting security controls in place, such as disaster recovery plans, business continuity management, and incident response plans. The technical context evaluated the organization's current technological infrastructure and capabilities as well as the intrinsic features of the technology within the Technology-Organization-Environment (TOE) framework [59].

By incorporating resilience as a variable, the study evaluated the technological preparedness of Ethiopian fintech companies to effectively respond to and recover from cybersecurity incidents. This included assessing factors such as the availability of redundant systems, data backup and recovery mechanisms, and incident response procedures. The study aimed to examine how technological factors influenced cybersecurity readiness and how well organizations could maintain operations and protect critical assets in the event of a cyber attack or breach.

Theoretical Basis:

- NIST CSF: The "Recover" function emphasizes resilience by ensuring that an organization can restore capabilities or services impaired during a cybersecurity incident. Resilience involves planning and preparedness to sustain operations under adverse conditions.
- ISO/IEC 27001: Includes requirements for business continuity management and incident response, focusing on resilience to ensure that organizations can recover from disruptions quickly.

(c) **Competency**
Competency referred to the knowledge, skills, and expertise of the staff responsible for implementing and managing cybersecurity within an organization. It also included the availability of training programs and resources aimed at improving cybersecurity capabilities. In the Technology-Organization-Environment (TOE) framework, the organizational context involved factors like human resources, organizational culture, and management support [59]. The environmental context considered external factors, such as industry trends, regulations, and the availability of skilled labor [60].

In this study, competency was used to assess how human capital and knowledge management influenced cybersecurity readiness in Ethiopia's fintech sector. The analysis covered aspects like the availability of skilled cybersecurity professionals, employee training and awareness programs, collaboration and knowledge-sharing among staff, and the organization's ability to attract and retain talent. The study also examined the external context by considering the role of industry best practices, regulatory requirements, and access to external resources or partnerships that supported the development of cybersecurity skills.

Theoretical Basis:

- NIST CSF: The "Protect" and "Respond" functions include aspects related to training and awareness programs, as well as the skills and expertise required to implement protective measures and respond to incidents effectively.
- ISO/IEC 27001: Emphasizes the need for competency through continuous training, awareness, and education programs to ensure that employees are knowledgeable about information security practices.
- Industry Reports: Reports by organizations like International Information System Security Certification Consortium underscore the importance of a competent cybersecurity workforce in managing and mitigating cyber risks.

2. **Dependent Variable**

(a) **Preparation**
Using the three independent variables, the study measured the cybersecurity readiness of Ethiopia's fintech ecosystem, with preparedness being the dependent variable. This assessment enabled a close evaluation of the sector's present cybersecurity status and identify gaps. The dependent variable, cybersecurity readiness, encompasses several crucial factors, including:

- The quality and effectiveness of security measures and controls implemented.
- Compliance with relevant cybersecurity laws and regulations. The ability to maintain operations and recover swiftly after a cyber attack.
- Awareness and understanding of both current and emerging cyber threats.
- The capacity to build and maintain customer trust through data protection.
- The efforts made toward innovation and adopting new cybersecurity solutions and technology.
- The maturity and development of cybersecurity practices within organizations.

This approach enables a comprehensive assessment of the sector's cybersecurity preparedness, highlighting areas for improvement and tackling major challenges.

Theoretical Basis:

- NIST CSF: The "Protect" and "Detect" functions collectively ensure that an organization is prepared to handle cybersecurity threats through proactive measures and continuous monitoring.
- ISO/IEC 27001: Preparation involves implementing controls identified in the risk assessment process to mitigate potential cybersecurity threats, ensuring that the organization is ready to respond to incidents.
- Best Practices: Frameworks like COBIT 5 and NIST SP 800-53 highlight preparation as a key component of cybersecurity, focusing on proactive risk management and incident response planning.

The use of the TOE framework not only ensures a structured approach to variable selection but also aligns the study with a well-established theoretical model, enhancing the rigor and relevance of the research findings.

3.2.3 Study Population & Sampling

The study population was divided into two primary groups within the fintech ecosystem to ensure the inclusion of all relevant stakeholders. This approach was designed to capture diverse perspectives and ensure comprehensive participation, thereby enhancing the quality and reliability of the research findings.

Regulatory agencies in charge of monitoring, controlling, and guaranteeing adherence to cybersecurity regulations and standards in the fintech sector made comprised the initial group of attendees. This group comprised institutions including the Ministry of Innovation and Technology (MiNT), the Financial Intelligence Center (FIC), the Information Network Security Agency (INSA), and the National Bank of Ethiopia (NBE). These organizations are essential in establishing regulations and implementing laws that safeguard the fintech sector against new online dangers [32].

The other group comprised organizations within the financial sector leveraging technology, including traditional financial institutions, payment processors, payment gateways, fintech companies, and telecom operators. Participants in this study included Commercial Bank of Ethiopia (CBE), EthSwitch, Abay Bank, Tsehay Bank, Buna Bank, Ahadu Bank, Ethio Telecom, Safaricom, AddisPay, Kacha, and Kifiya Financial Technology.

To ensure a targeted and effective selection of participants, a purposive sampling method was employed, focusing on companies and organizations with extensive knowledge and experience in Ethiopia's fintech industry. This approach was specifically designed to gather insights that directly addressed the research questions.

The study made sure that the sample was in a prime position to offer insightful information on current cybersecurity practices, pinpoint important readiness gaps, and aid in the creation of a useful cybersecurity assessment instrument by choosing these knowledgeable stakeholders. The overall relevance and validity of the study's findings are improved by this connection between the sampling strategy and the research topics.

3.2.4 Data Collection

Data was collected from two groups of participants using structured questionnaires designed to address the research questions through four variables: governance, resilience, competency, and preparedness. Two separate sets of questionnaires were prepared for fintech companies and regulatory bodies.

The research methodology included the preparation of two tailored questionnaires: one directed at regulatory bodies and the other at fintech companies. The questionnaire for regulatory bodies comprised 28 questions, while the one for fintech companies contained 27 questions. These instruments were distributed via Google Forms and through direct visits to the identified organizations. Both sets of questions were specifically designed to align with the respective variables and contribute to answering the study's research questions.

3.2.5 Quantitative Instrument

This research utilized quantitative data collection through a structured questionnaire and purposive sampling. Participants were selected based on their involvement in the fintech sector and related businesses.

Structured Questionnaire: The data was collected from two categories of participants, as previously mentioned. Separate questionnaires were prepared to address the research questions according to each participant's role in the industry. Regulatory bodies were given 28 questions, and 20 participants responded. Meanwhile, fintech companies were asked 27 questions, with 40 participants positively returning their questionnaires. The questionnaires were distributed through two channels: Google Forms and paper-based surveys. In addition to research-specific questions, demographic questions were included to analyze the distribution of professionals in the industry.

3.2.6 Data Validation and Expert Consultation

A number of steps were taken to guarantee the quality and dependability of the research tools before any data was collected. These procedures were intended to ensure that the information collected would be reliable and consistent, improving the overall standard and reliability of the findings of the investigation.

- Pilot Testing: A small sample of individuals from the target population took part in a pilot test. This made it possible to improve the questionnaire and guarantee that the questions were appropriate, pertinent, and clear. Pilot test feedback aided in locating any unclear or ambiguous elements that would jeopardize the validity of the data.
- Expert Review: The research instruments, including questionnaires, were reviewed by cybersecurity and research methodology experts. Their insights helped in fine-tuning the questions to better align with the research objectives and variables. This step ensured that the instruments were capable of capturing accurate and meaningful data relevant to cybersecurity readiness.
- Reliability Testing: A reliability analysis was carried out utilizing techniques like Cronbach's alpha to determine internal consistency of the questionnaire items to ensure consistency in responses.This stage contributed in assessing the extent to which the questionnaire's items produced reliable and consistent outcomes or unclear items that can damage the quality of the data
- Validation of Content: Content validity was achieved by aligning the questionnaire items with established frameworks and best practices in cybersecurity. This alignment ensured that the questions covered all critical aspects of the research variables and were grounded in theoretical and practical foundations.
- Clear Instructions: Detailed and unambiguous instructions were provided to the respondents to minimize any potential misinterpretation of the questions. This step further strengthened the accuracy of the data collected.

Through the application of validation and reliability procedures, the study ensured the collected data was of high quality, thereby strengthening the credibility of the research findings.

3.2.7 Data Analysis

After cleaning and compiling the data, analysis was performed using IBM SPSS Statistics software, version 23. Descriptive analyses were applied to summarize the data, including calculating frequencies and percentages for discrete variables, means and standard deviations for symmetrically distributed variables, and medians and ranges for variables with non-symmetrical distributions. This approach provided a comprehensive overview of the dataset, facilitating an accurate interpretation of the research findings.

3.2.8 Ethical Considerations

The study complied with ethical guidelines to guarantee the preservation of participants' rights and the integrity of the research process. Before the collection of data, all participants gave their consent after being fully informed about the study's objectives and the confidentiality of their answers. To respect their autonomy, participants were made aware of their freedom to leave the study at any moment and without consequence.

Written consent was also obtained, ensuring transparency and accountability in the data collection process. Care was taken to design questionnaires that avoided culturally sensitive, inappropriate, or intrusive questions. No confidential organizational information was requested, ensuring that participants could respond without concerns about compromising their company's data security.

To further protect participants, the study ensured anonymity where appropriate, and data was handled in a secure and confidential manner throughout the research process. In addition to that, the research complied with data protection laws, ensuring that all collected information was securely stored and accessible only to the research team for analysis. Any potential conflicts of interest were disclosed, and the study maintained transparency and fairness in reporting its findings.

4 Result And Discussion

4.1 Introduction

This section presents the quantitative data collected between May 1 and May 30, 2024, from two distinct participant groups selected for this study. The analysis was divided into two main parts.

The first part focused on basic demographic details of the participants, such as age, gender, and work experience in the fintech industry. The following section highlighted the finding of the research topic. The quantitative data was effectively displayed through tables and graphs using various statistical methods.

A total of 60 participants were selected for this study, with 40 from fintech companies and 20 from regulatory bodies. A purposive sampling method was used to ensure that the participants held key roles in cybersecurity or related functions. While the sample size captures diverse perspectives, it may limit the generalizability of the findings. A larger, more stratified sample could provide additional insights into the sector's cybersecurity practices.

4.2 Demographic Characteristics Of Respondents

In this section of the results and discussion, it presented and analyzed the demographic distribution of the research participants, focusing on variables such as age, gender, and work experience. Through examining these dimensions, the research obtained an overview of the demographic distribution of cybersecurity professionals in the fintech arena, which guided further study and investigation to impact the overall cybersecurity practice.

The workforce composition was notably revealed by the examination of age, gender, and work experience; this, in turn, impacted the industry's capacity to address cybersecurity risks. The age distribution, for example, showed a mix between younger, possibly more tech-savvy workers and seasoned experts. The distribution of genders was equally significant because diversity in the workforce may lead to a wider range of viewpoints and methods for addressing cybersecurity issues.

Additionally, the degree of industry competence was indicated by work experience. We were able to evaluate the possible influence of this expertise on the sector's preparedness and resilience by knowing the number of experts with different levels of experience. It was possible to make links between the workforce's traits and the industry's readiness to deal with risks related to cybersecurity by analyzing these demographic aspects.

This analysis not only provided a snapshot of the then-current state of the cybersecurity workforce but also offered insights into areas where improvements might have been necessary.

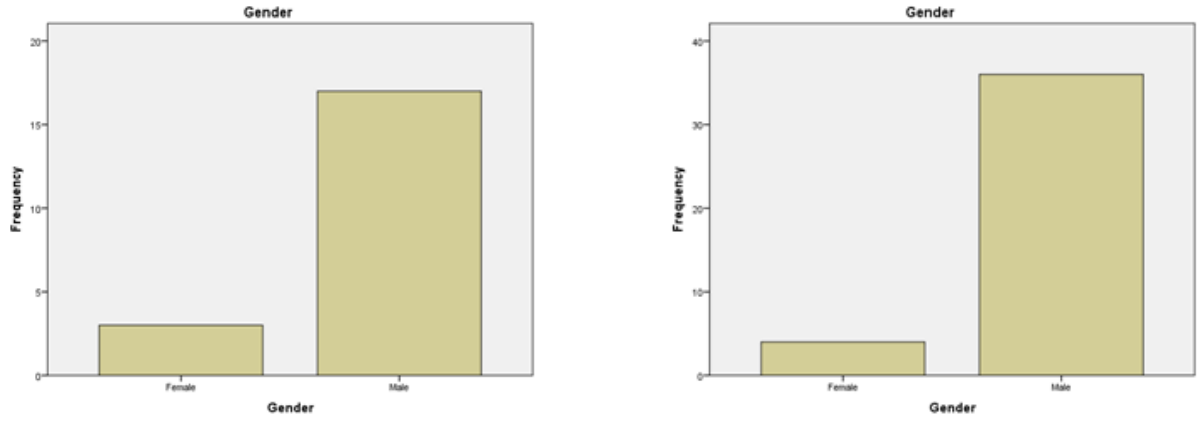
4.2.1 Gender Distribution Insights

This study had collected data on gender to understand the distribution within the cybersecurity profession in fintech companies. The findings reveal a clear gender disparity, with the majority of participants being male, indicating that the industry is predominantly male-dominated.

This gender imbalance suggested a need for further research to explore the underlying reasons and potential impacts of such a gap. Investigating the causes of gender imbalance in cybersecurity roles could provide insights into the barriers that women faced in entering and advancing within the field.

4.2.2 Age Distribution In Cybersecurity Profession In Fintech

The analysis of age distribution within the cybersecurity profession in fintech companies shows that this field is still developing in Ethiopia's digital business landscape. The data reveals that a notab portion of cybersecurity professional's fall within the 31-40 age range. This concentration suggests that the profession is gaining traction and is recognized as essential in the current digital era. Many of the participant in this age group hold managerial positions in their respective organizations.



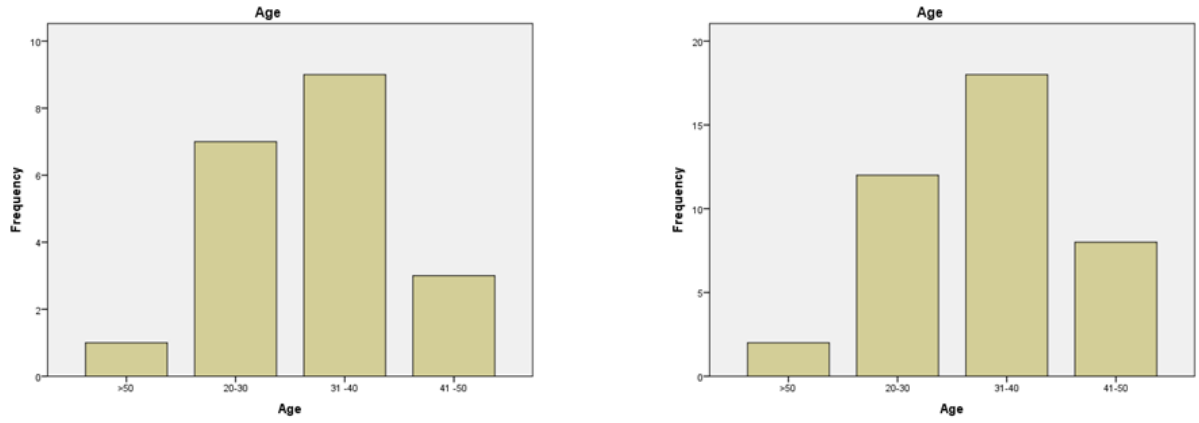
(a) Gender in Regulator

(b) Gender in Fintech Company

Figure 2: Gender Distribution In Cybersecuirty

The presence of a noticeable number of professionals in the 20-30 age range indicates that younger individuals are increasingly pursuing careers in cybersecurity.

The smaller representation in the 41-50 and ¿50 age groups suggests that cybersecurity is a newer field within the region, with fewer late-career professionals having transitioned into this area. This age distribution highlights the growing recognition of cybersecurity's importance and the increasing interest among younger professionals in pursuing careers in this field.



(a) Regulator

(b) Fintech Company

Figure 3: Comparison of Age Distribution

4.2.3 Work Experience Distribution

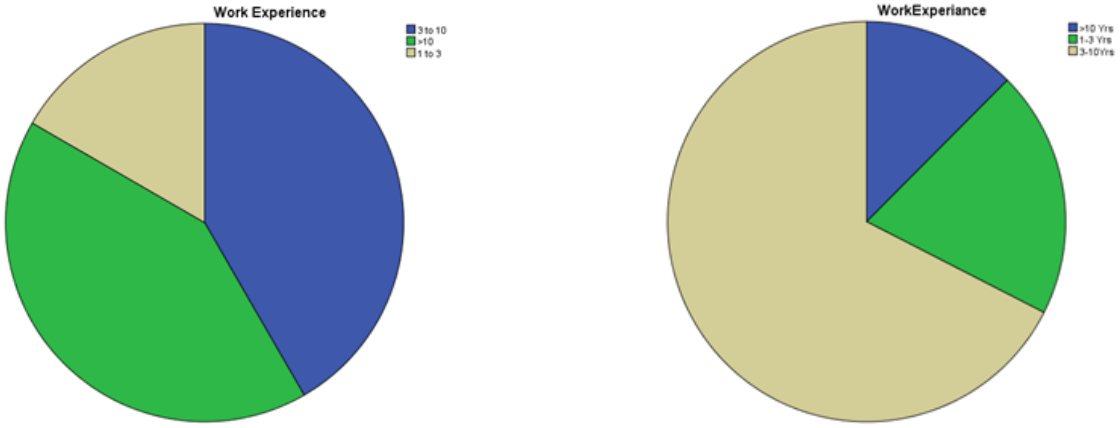
The data reveals that the majority of participants (60%) have 3 to 10 years of work experience, as shown by the blue segment in the pie chart.

On the other hand, 35% of participants have over 10 years of experience, representing a substantial group of seasoned professionals with deep industry knowledge. Meanwhile, 5% of participants have 1 to 3 years of experience, introducing fresh ideas and contemporary skills to the industry.

It is important to note that this study does not assess the participants' understanding, expertise level, academic competency, or specific skill sets, particularly in the domain of cybersecurity. These aspects could be potential areas for future research to better identify the required skills and expertise in specific

domains.

Overall, the balanced distribution of work experience among participants highlights the strength of fintech companies in leveraging both experienced professionals and newer talent for dynamic and innovative work environment. This mix is advantageous, as it combines the deep industry knowledge of seasoned professionals with the fresh perspectives of newer employees, ensuring a comprehensive approach to addressing challenges within the fintech industry.



(a) Regulator (b) Fintech Company

Figure 4: Analysis of Work Experience

4.3 Cybersecurity Readiness Analysis

4.3.1 ANOVA and Regression Analysis Explanation

A statistical technique called **ANOVA (Analysis of Variance)** is used to ascertain whether the means of three or more groups differ in ways that are statistically significant.For trials involving complicated data sets, this approach proves essential because it delivers more accurate and trustworthy outcomes [79]. ANOVA is used in this study to determine whether the independent factors (resilience, competency, and governance) have a significant effect on the cybersecurity readiness of fintech companies and regulatory agencies.

In regression analysis, ANOVA is used to test whether any of the independent variables have a significant effect on the dependent variable by comparing the variability explained by the model to the unexplained variability (residuals)[62].

Regression Analysis is a statistical technique used to model the relationship between a dependent variable and one or more independent variables. In this case, it helps quantify how Governance, Competency, and Resilience influence the cybersecurity preparedness of both regulatory bodies and fintech companies.

The combined use of ANOVA and Regression provides both an understanding of the overall influence of the independent variables and a detailed examination of the contribution of each variable to cybersecurity preparedness.

4.3.2 Regulatory Bodies Cybersecurity Readiness

Regulatory bodies are responsible for maintaining a secure fintech ecosystem by implementing policies and enforcing compliance. This analysis evaluates their cybersecurity readiness by focusing on Governance (GFR), Competency (CFR), and Resilience (RFR), and their collective effect on Preparedness (PFR).

Table 1: Variables Entered/Removed For Regulator

Model	Variables Entered	Variables Removed	Method
1	CFR, GFR, RFR[b]	.	Enter
a Dependent Variable: PFR			
b All requested variables entered.			

Table 2: Model Summary For Regulator

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.998[a]	.995	.994	.04706
a Predictors: (Constant), CFR, GFR, RFR				

Analysis of Variance for Regulator:

The ANOVA test shows a high F-statistic (1069.082) and a p-value < 0.001, indicating that the independent variables (GFR, CFR, RFR) have a statistically significant impact on the dependent variable (PFR).

R-square = 0.995 means that 99.5% of the variance in PFR is explained by GFR, CFR, and RFR.

Table 3: ANOVA For Regulator

Model	Sum of Squares	df	Mean Square	F	Sig.
1 (Regression)	7.102	3	2.367	1069.082	0.000[b]
(Residual)	0.035	16	0.002		
(Total)	7.137	19			
a Dependent Variable: PFR					
b Predictors: (Constant), CFR, GFR, RFR					

The F-statistic of 1069.082 and a p-value of less than 0.001 show that the regression model is statistically significant. This implies that the model's occurrence is extremely unlikely to have been accidental. Statistical significance is generally indicated by a p-value of less than 0.05. In this instance, there is substantial evidence against the null hypothesis because the p-value is significantly smaller than 0.05 (in fact, less than 0.001). This indicates that the independent factors (GFR, CFR, and RFR) together significantly affect the dependent variable (PFR).

The high F-statistic (1069.082) indicates that the variance explained by the regression model is significantly greater than the variance unexplained (or residual variance). This implies that the model with the predictors (GFR, CFR, and RFR) fits the data much better than a model without these predictors. Essentially, the F-statistic measures the overall significance of the regression model. A high F-value, combined with a low p-value, signifies that the model provides a much better fit to the data compared to a model with no predictors.

The F-test in regression analysis examines whether a group of independent variables, taken together, meaningfully impacts the dependent variable. A positive F-test result indicates that these variables, collectively, contribute to explaining the variations in the dependent variable (PFR)[53]. This highlights the importance of governance, competency, and resilience as key factors influencing cybersecurity preparedness, and their combined effect is statistically significant.

In general, the ANOVA results demonstrate that the regression model used in this study is highly effective in predicting the cybersecurity preparedness of regulatory bodies. The significant F-statistic and the very low p-value indicate that the selected independent variables (GFR, CFR, RFR) are important predictors. This reinforces the validity of the model and underscores the importance of governance, competency, and resilience in enhancing cybersecurity readiness. The findings suggest that improving

these factors can lead to better cybersecurity outcomes for regulatory bodies in the fintech ecosystem.

Regression Analysis For Regulator:

The regression model aims to understand the relationship between the independent variables (GFR, CFR, RFR) and the dependent variable (PFR).

Table 4: Coefficients For Regulator

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
1 (Constant)	0.132	0.070		1.892	0.077
RFR	0.530	0.095	0.519	5.592	0.000
GFR	0.272	0.078	0.291	3.478	0.003
CFR	0.180	0.067	0.197	2.665	0.017
a Dependent Variable: PFR					

Constant (Intercept): The constant represents the expected value of the dependent variable PFR when all independent variables (GFR, CFR, RFR) are zero. Here, the coefficient of 0.132 indicates that when GFR, CFR, and RFR are zero, PFR is expected to be 0.132. However, since the significance value is 0.077 (greater than 0.05), the constant is not statistically significant. This means the intercept does not provide a meaningful contribution to the model [61].

Resilience (RFR) has the strongest positive influence on preparedness, with a coefficient of 0.530 ($p < 0.001$).The unstandardized coefficient of 0.530 means that for every one-unit increase in RFR, PFR increases by 0.530 units, all else being equal. The standardized coefficient (Beta) of 0.519 indicates that RFR has the strongest positive effect among the predictors. The t-value of 5.592 with a significance level of 0.000 shows that RFR is highly significant ($p < 0.05$), indicating that resilience is a vital factor in enhancing cybersecurity preparedness.

Additionally, preparation is highly impacted by Governance (GFR), with a value of 0.272 ($p = 0.003$).Assuming all other factors remain constant, the unstandardized coefficient of 0.272 indicates that PFR rises by 0.272 units for every unit increase in GFR. In comparison to other predictors in the model, GFR has a significantly positive impact, as indicated by the standardized coefficient (Beta) of 0.291. With a significance level of 0.003, the t-value of 3.478 indicates that this variable is highly significant (p ¡ 0.05), indicating that governance plays a critical role in assessing cybersecurity readiness.

Competency (CFR) has a smaller but significant effect, with a coefficient of 0.180 ($p = 0.017$). The unstandardized coefficient of 0.180 implies that for every one-unit increase in CFR, PFR increases by 0.180 units, holding other variables constant. The standardized coefficient (Beta) of 0.197 shows that CFR has a relatively smaller effect compared to GFR. The t-value of 2.665 with a significance level of 0.017 indicates that CFR is statistically significant ($p < 0.05$), suggesting that competency is an important factor in cybersecurity preparedness.

Overall Result Analysis

The analysis results revealed that all three independent variables—governance (GFR), competency (CFR), and resilience (RFR)—played a significant role in influencing cybersecurity preparedness (PFR). Among these factors, resilience (RFR) had the greatest impact, followed by governance (GFR) and competency (CFR). The importance of these variables emphasizes their key role in shaping the readiness of regulatory bodies to handle cybersecurity challenges. The model suggests that strengthening governance structures, enhancing skill levels, and improving resilience would lead to notable improvements in overall cybersecurity preparedness.

4.3.3 Fintech Companies Cybersecurity Readiness

Fintech companies are particularly vulnerable to cybersecurity risks due to their reliance on digital platforms. This analysis evaluates their cybersecurity readiness by focusing on Governance (GFC),

Competency (CFC), and Resilience (RFC), and their combined effect on Preparedness (PFC).

Table 5: Variables Entered/Removed For Fintech Company

Model	Variables Entered	Variables Removed	Method
1	GFC, CFC, RFC[b]	.	Enter
[a] *Dependent Variable: PFC*			
[b] *All requested variables entered.*			

Table 6: Model Summary Fintech Company

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.998[a]	.996	.996	.05548
[a] *Predictors: (Constant), GFC, CFC, RFC*				

Analysis of Variance For Fintech Companies :

The ANOVA test yields a high F-statistic (3023.358) and a p-value < 0.001, indicating that the independent variables (GFC, CFC, RFC) significantly influence the dependent variable (PFC).
R-square = 0.996 means that 99.6% of the variance in PFC is explained by the independent variables.

Table 7: ANOVA For Fintech Company

Model	Sum of Squares	df	Mean Square	F	Sig.
1 CRegression)	27.914	3	9.305	3023.358	0.000[b]
(Residual)	0.111	36	0.003		
(Total)	28.025	39			
a Dependent Variable: PFR					
b Predictors: (Constant), GFC, CFC, RFC					

The ANOVA table offers several key insights into the effectiveness of the regression model:

27.914 is the regression's Sum of Squares (SS), which indicates the proportion of the dependent variable's variation that can be explained by the independent variables in the model. This chart shows how effectively the model can account for variations in the dependent variable as the independent factors change.

The number of independent variables in the model is represented by the regression's Degrees of Freedom (df), which is 3. Because they represent the quantity of independent pieces of information available to estimate parameters, degrees of freedom are significant.

The Mean Square (MS) for the regression is 9.305, calculated by dividing the regression sum of squares by the degrees of freedom. This value represents the average amount of variation explained by each independent variable in the model. Specifically, it is computed as::

$$\text{MS}_{\text{regression}} = \frac{27.914}{3} = 9.305$$

The F-statistic is 3023.358, which is the ratio of the mean square of the regression to the mean square of the residuals. A high F-value indicates that the model explains a significant portion of the variance in the dependent variable. This suggests that the independent variables, when taken together, have a strong and statistically significant impact on the dependent variable.

The Significance (Sig.) level is 0.000, indicating the probability that the observed F-statistic would occur if the null hypothesis (which states that the independent variables have no effect) were true. A p-value of 0.000 strongly suggests that it is highly unlikely the null hypothesis is true, meaning the regression model is statistically significant. This low p-value confirms that the results are not due to random chance, and the independent variables significantly affect the dependent variable.

For the residuals, the sum of squares is 0.111, representing the variation in the dependent variable that is not explained by the model. The residual degrees of freedom is 36, calculated as the total number of observations minus the number of independent variables and one ($39 - 3 - 1 = 36$). The mean square for the residuals is 0.003, derived by dividing the residual sum of squares by the residual degrees of freedom:

$$\text{MS}_{\text{residual}} = \frac{0.111}{36} = 0.003$$

The total sum of squares is 28.025, which is the sum of the regression sum of squares and the residual sum of squares ($27.914 + 0.111 = 28.025$). The total degrees of freedom is 39, calculated as the total number of observations minus one. This represents the overall variation in the dependent variable, encompassing both explained and unexplained variation.

The total sum of squares is 28.025, which is the sum of the regression sum of squares and the residual sum of squares ($27.914 + 0.111 = 28.025$). The total degrees of freedom is 39, calculated as the total number of observations minus one. This represents the overall variation in the dependent variable, encompassing both explained and unexplained variation.

Regression Analysis For Fintech Company:

Constant (Intercept): The constant represents the expected value of the dependent variable PFC when all independent variables (RFC, CFC, GFC) are zero. Here, the coefficient of 0.033 indicates that when RFC, CFC, and GFC are zero, PFC is expected to be 0.033. However, since the significance value is 0.320 (greater than 0.05), the constant is not statistically significant. This means the intercept does not provide a meaningful contribution to the model.

Resilience (RFC): With a coefficient of 0.473 ($p < 0.001$), resilience (RFC) is the most important component. This means that improving preparedness has the biggest influence; if all other factors remain constant, PFC rises by 0.473 units for every unit increase in RFC. The standardized coefficient (Beta) of 0.469 indicates that RFC has a significant positive effect relative to other predictors in the model. GFC is quite significant ($p < 0.05$), as indicated by the t-value of 5.295 at a significance level of 0.000, suggesting that governance is essential to improving cybersecurity readiness.

Governance (GFC) has a substantial positive impact on PFC the unstandardized coefficient of 0.401 means that for every one-unit increase in GFC, PFC increases by 0.401 units, all else being equal. The standardized coefficient (Beta) of 0.400 indicates that GFC has a significant positive effect, almost as strong as RFC. GFC is extremely significant ($p <0.05$), as indicated by the t-value of 5.295 at a significance level of 0.000, suggesting that governance is essential to improving cybersecurity readiness.

Competency (CFC) has a smaller but statistically significant effect, with a coefficient of 0.134 ($p = 0.045$). The unstandardized coefficient of 0.134 implies that for every one-unit increase in CFC, PFC increases by 0.134 units, holding other variables constant. The standardized coefficient (Beta) of 0.133 shows that CFC has a relatively smaller effect compared to RFC. The t-value of 2.079 with a significance level of 0.045 indicates that CFC is statistically significant ($p < 0.05$), suggesting that competency is an important factor in cybersecurity preparedness.

Overall Result Analysis

The results for fintech companies indicate that all three independent variables (RFC, CFC, GFC) significantly contribute to the dependent variable (PFC), with resilience (RFC) having the strongest influence, followed by governance (GFC), and then competency (CFC). The statistical significance of these variables highlights their importance in determining the cybersecurity readiness of fintech companies. The model

Table 8: Coefficients For Fintech Company

Model		Unstandardized Coefficients	Standardized Coefficients	t	Sig.
		B	Std. Error	Beta	
1 .320	(Constant)	.033	.033		1.008
.000	RFC	.473	.072	.469	6.559
.045	CFC	.134	.065	.133	2.079
.000	GFC	.401	.076	.400	5.295
[a] *Dependent Variable: PFC*					

suggests that improving resilience, governance, and competency can significantly enhance cybersecurity preparedness.

4.4 Consolidated Analysis Of Fintech Cybersecurity Preparedness

This section of the analysis presents the study's findings, offering a detailed exploration of how governance, competency, and resilience influence cybersecurity preparedness in both regulatory bodies and fintech companies. The research demonstrates that these selected variables are effective in measuring the strengths and weaknesses of cybersecurity readiness within Ethiopia's fintech ecosystem. The methodology employed in this study provided a clear view of how these factors impact the overall cybersecurity preparedness of the sector.

The data collection and analysis were conducted separately for the two key groups—regulatory bodies and fintech companies. However, the consolidated analysis highlights how the independent variables (governance, competency, and resilience) significantly influence the dependent variable, cybersecurity readiness. This provides critical insights into the state of cybersecurity in the fintech ecosystem, revealing the essential components necessary to improve cybersecurity measures.

According to the R-square values, the investigation shows that both regulators and fintech businesses have high levels of explanatory power. It means that resilience, competence, and governance play an integral part in assessing cybersecurity readiness throughout the industry.

For regulatory bodies, resilience (RFR) emerged as the most impactful factor, emphasizing the importance of being able to recover from cyber incidents. Governance (GFR) and competency (CFR) also play significant roles, although to a slightly lesser extent. In contrast, within fintech companies, both resilience (RFC) and governance (GFC) were key drivers of cybersecurity preparedness, although governance appeared to have a stronger influence compared to its role in regulatory bodies.

The alignment of these findings between regulatory agencies and fintech companies underscores the importance of governance. According to [66] "Cyber governance is a critical part of modern cybersecurity regimes in finance. The evidence from the study reveals that effective governance practices not only within regulatory bodies but also within fintech companies are essential to improve cybersecurity readiness and resilience in the digital financial sector. By analyzing the interaction between regulatory oversight and industry practices, the study highlights how cohesive governance frameworks can promote a more secure environment against cyber threats and breaches.

4.4.1 Examine Existing Practices

The research successfully investigated current cybersecurity practices by identifying the current state of cybersecurity efforts within fintech companies and regulatory bodies in Ethiopia. It aligned well with the first specific objective by examining key areas such as governance frameworks, resilience-building initiatives, and the development of cybersecurity competencies.

Although the study revealed that many organizations lack formalized cybersecurity policies, Ethiopian fintech companies are recommended to adopt structured frameworks such as NIST CSF or ISO/IEC 27001. Implementing these frameworks could improve governance structures, incident response, risk management, and overall cybersecurity resilience. Furthermore, providing real-world examples of how these frameworks are used in other countries would offer a valuable benchmark for Ethiopian fintech companies to align their practices with international standards.

4.4.2 Gaps in Cybersecurity Readiness

The research addressed the second objective by identifying gaps within Ethiopia's fintech industry. The findings revealed deficiencies in governance, particularly in areas such as risk management and regulatory compliance. One major issue was the inability of regulators to effectively enforce cybersecurity policies.

Another weakness identified was resilience. Many fintech companies struggled to implement effective incident response plans and business continuity plans. Unlike international best practices—such as ISO/IEC 27001 and NIST SP 800-61—which provide comprehensive guidelines for incident response and continuity planning, Ethiopian fintech companies lack the formal structures recommended by these frameworks. Encouraging the adoption of such standards could greatly enhance the sector's overall resilience.

Moreover, the study highlighted gaps in competency across the ecosystem, including a shortage of skilled cybersecurity professionals and a lack of awareness, collaboration, and communication. Global initiatives like the NICE Cybersecurity Workforce Framework [78] emphasize the importance of building cybersecurity competency through structured training and development programs.

4.4.3 Evaluate cybersecurity readiness and posture of fintech companies

The research results met the third objective, which set to evaluate cybersecurity readiness and maturity within the Ethiopian fintech sector. The ANOVA and regression analysis models provided a clear quantitative assessment of the sector's readiness. The findings showed that governance, competency, and resilience are the three critical factors that strongly influence the overall cybersecurity readiness.

Governance:

The analysis indicated that governance frameworks significantly impact the ability of fintech companies and regulatory bodies to manage cybersecurity risks effectively. Companies with structured governance practices demonstrated better readiness in dealing with cyber threats.

Competency:

The research revealed that the skill level and knowledge of cybersecurity professionals within organizations also play a major role in determining readiness. Organizations that invest in cybersecurity training and awareness programs showed higher levels of maturity in their security practices.

Resilience:

Perhaps the most striking finding from the statistical models was the role of resilience. Companies that had an incident response plans, business continuity measures, and cyber risk management frameworks were better equipped to recover from cyber incidents and maintain their operations.

The statistical models ANOVA and regression analysis, demonstrated that these three factors—governance, competency, and resilience—accounted for a significant portion of the variability in cybersecurity readiness. This shows that improving these areas could lead to substantial gains in the sector's cybersecurity maturity.

4.4.4 Proposed Practical Cybersecurity Assessment Tool

The research has clearly identified several gaps in cybersecurity governance, competency, and resilience within Ethiopia's fintech sector. Based on these findings, this study proposes a tailored cybersecurity assessment tool designed to address these gaps. The primary goal of this tool is to evaluate the cybersecurity readiness of both fintech companies and regulatory bodies, while offering practical, actionable

steps to strengthen their cybersecurity postures. The proposed tool serves as a foundational resource, helping to improve cybersecurity readiness at both the organizational and sectoral levels.

The proposed tool is built upon international cybersecurity frameworks such as NIST CSF, ISO/IEC 27001, and the FFIEC Cybersecurity Assessment Tool, but adapted to the specific needs and constraints of the Ethiopian fintech sector. This ensures that the tool not only follows globally recognized best practices but also considers local challenges such as resource limitations, lack of skilled professionals, and regulatory gaps.

- Governance: The tool assesses the presence and strength of governance structures within organizations, focusing on risk management, policy development, and regulatory compliance. By establishing a clear governance framework, organizations can better manage cybersecurity risks and align with international standards.
- Competency: The tool evaluates the level of cybersecurity knowledge, awareness, and skills within the organization. It provides a structured pathway for training programs and capacity-building initiatives, enabling companies to bridge the skills gap. Drawing from the NICE Cybersecurity Workforce Framework, the tool emphasizes continuous professional development in the face of evolving cyber threats.
- Resilience: The tool measures an organization's ability to respond to, recover from, and adapt to cybersecurity incidents. It provides guidance on building business continuity plans, incident response frameworks, and disaster recovery protocols, ensuring that fintech companies can quickly restore operations after a cyber incident.

One of the key features of this tool is its adaptability to the local context. The Ethiopian fintech industry faces unique challenges, including limited resources, lack of infrastructure, and fragmented regulatory oversight. Therefore, the tool is designed to be scalable and flexible, allowing both large and small fintech companies to implement cybersecurity measures in accordance with their capabilities. For instance, the tool can help startups by offering cost-effective and easy-to-implement solutions that don't compromise on security standards.

In addition to addressing technical aspects, the tool focuses heavily on a cybersecurity-aware culture within organizations. One of the research findings was the lack of awareness and inadequate communication about cybersecurity threats. By embedding cybersecurity awareness programs into the assessment tool, the goal is to educate employees and stakeholders on the importance of security protocols.

A more educated workforce means that companies well equipped to identify and mitigate cyber threats before they escalate into critical incidents. By promoting regular cybersecurity training and encouraging cross-sector collaboration, the tool supports the creation of an industry-wide security culture.

The tool is designed not only to assess current cybersecurity practices but also to encourages continuous improvement. Companies and regulators can use the tool to conduct regular assessments, track their progress, and adapt to emerging threats. As the cyber threat landscape evolves, so too can the assessment criteria, ensuring that Ethiopian fintech companies remain resilient and prepared for future challenges.

Further more, the tool encourages collaboration between regulators and fintech companies, facilitating information-sharing and joint initiatives to address common threats. A unified approach ensures that both regulatory bodies and businesses move toward the same goals in terms of cybersecurity standards and compliance.

Finally, the cybersecurity assessment tool proposed in this research provides a practical, adaptive, and forward-thinking solution to the challenges identified in Ethiopia's fintech sector. It offers a roadmap for strengthening governance, improving skills, and building resilience, ensuring that the sector can withstand the growing threat of cyberattacks. This tool is essential for establishing a secure financial ecosystem in Ethiopia, one that cultivate trust, growth, and sustainability.

Proposed Cybersecurity Assessment Tool

Domain 1: Governance

Category	Sub-Category	Requirements	Sources/Map to International Standards
Risk Management	Risk Identification	• Identify and catalog critical assets, including data, systems, and hardware. • Continuously identify and document potential threats and vulnerabilities. • Assess the cybersecurity readiness of third-party vendors and partners.	• NIST CSF: ID.AM-1, ISO/IEC 27001: A.8.1 • NIST CSF: ID.RA-1, ISO/IEC 27001: A.8.2 • ISO 31000, NIST SP 800-30
	Risk Assessment and Analysis	• Evaluate the likelihood of identified risks and their potential impact. • Prioritize risks based on severity. • Ensure risk assessments comply with laws and regulations (e.g., GDPR, PSD2).	• NIST SP 800-30, ISO/IEC 27001: A.8.2.1 • NIST CSF: ID.RA-5, ISO/IEC 27001: A.18.1
	Risk Mitigation and Control	• Develop and implement treatment plans for identified risks. • Ensure incident response and recovery mechanisms are in place.	• NIST SP 800-30, NIST CSF: ID.RA-6, ISO/IEC 27001: A.8.3 • NIST CSF: PR.IP-9, ISO/IEC 27002: A.16.1
Compliance	Regulatory Requirements	• Stay informed about evolving regulations (GDPR, PSD2, PCI-DSS). • Ensure timely reporting of cybersecurity incidents to regulators. • Ensure all Ethiopian regulatory compliance with INSA and NBE regulation and standard.	• NIST CSF: ID.GV-3, ISO/IEC 27001: A.18.1.1 • Critical Mass Cyber Security Requirement Standard Version 2.0

	Policy and Procedure Development	• Establish comprehensive governance policies to manage cybersecurity risks. • Ensure regular review of policies and provide employee training.	• ISO/IEC 27001: A.6 • NIST CSF: ID.GV-2
	Compliance Audits and Assessments	• Conduct regular internal and external cybersecurity audits. • Ensure third-party service providers undergo regular cybersecurity audits.	• ISO/IEC 27001: A.18.2.2, NIST CSF: ID.GV-1 • ISO/IEC 27001: A.15.2, NIST CSF: ID.SC-1
Asset Management	Asset & Inventory Management	• Classify assets based on sensitivity or criticality. • Define ownership, especially for customer data, and ensure accountability.	• NIST CSF: ID.AM-1, ISO/IEC 27001: A.8.1.1 • NIST CSF: ID.AM-2, ISO/IEC 27001: A.8.2.1 • NIST CSF: ID.AM-6, ISO/IEC 27001: A.8.1.2
	Configuration Management	• Maintain strict configuration baselines for financial systems. • Follow controlled change management processes.	• NIST CSF: PR.IP-1 • ISO/IEC 27001: A.12.1.2
Continuous Improvement and Monitoring	Performance Metrics and Measurement	• Establish metrics to measure the performance of cybersecurity programs.	• NIST CSF: PR.IP-12
	Continuous Monitoring	• Continuously monitor risks and review control effectiveness.	• NIST SP 800-30 • ISO/IEC 27002: A.18.2

Domain 2: Resilience

Category	Sub-Category	Requirements	Sources/Map to International Standards
Incident Management	Incident Detection and Reporting	• Use monitoring tools to detect unusual activities (e.g., unauthorized credit card use, suspicious API traffic). • Establish incident reporting mechanisms for data breaches. • Establish formal relationships with law enforcement agencies, national cybersecurity emergency response teams (CERTs), and relevant financial regulatory bodies to coordinate responses to significant cybersecurity incidents.	• FFIEC Cybersecurity Assessment Tool • ISO/IEC 27001: A.16.1.2
	Incident Response	• Establish incident response procedures and regularly test them.	• NIST SP 800-61, NIST CSF: RS.RP • ISO/IEC 27001: A.16.1.2
Business Continuity	Business Impact Analysis (BIA)	• Conduct BIAs to assess the impact of disruptions on critical services • Recovery priorities must be established based on the potential impact of service disruption, including financial losses, regulatory penalties, and reputational damage..	• FFIEC Reference: Resilience (Domain 5) • NIST CSF: ID.BE-5
	Business Continuity Plan (BCP)	• Establish BCPs to ensure rapid restoration of financial services. • Set Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	• ISO/IEC 27001: A.17.1.2, FFIEC Cybersecurity Assessment Tool: Incident Response and Business Resumption

Disaster Recovery	Disaster Recovery Plan (DRP)	• Maintain a formal DRP for IT systems and financial applications. • Regularly test disaster recovery plans.	• FFIEC Reference: Business Continuity Planning (Domain 5)
	Backup	• Ensure regular backups are conducted, and data can be restored to meet RPOs.	• FFIEC Reference: Backup and Recovery (Domain 4)
Vulnerability Management	Vulnerability Scanning	• Conduct regular vulnerability scans across the infrastructure. • Categorize vulnerabilities by risk severity.	• FFIEC Cybersecurity Assessment Tool: Vulnerability and Patch Management • NIST CSF: PR.IP-12
	Patch Management	• Establish a patch management policy to remediate identified vulnerabilities.	• FFIEC Cybersecurity Assessment Tool: Patch Management
	Third-Party Management	• Assess third-party service providers' security postures. • Conduct periodic audits of the supply chain to ensure compliance with Ethiopian regulation and international cybersecurity standards.	• FFIEC Reference: External Dependency Management (Domain 5) • ISO/IEC 27001

Domain 3: Competency

Category	Sub-Category	Requirements	Sources/Map to International Standards
Awareness and Training	Training Program Development	• Develop comprehensive cybersecurity awareness programs tailored to the fintech industry. • Ensure provided training on compliance with financial regulations (e.g.,Anti Money Laundering, Know Your Customer, GDPR).	• FFIEC Cybersecurity Assessment Tool • ISO/IEC 27001: A.7.2.3
	Awareness Campaigns	• Provide regular updates on new threats and best practices. • Evaluate the effectiveness of cybersecurity awareness programs.	• NIST CSF: PR.AT-1, FFIEC Cybersecurity Assessment Tool
Roles and Responsibilities	Role Definition and Assignment	• Clearly define cybersecurity roles and responsibilities. • Ensure relevant employees hold certifications (e.g., CISSP, CISM, CEH).	• FFIEC Reference: Governance (Domain 1) • ISO/IEC 27001: A.6.1.1
	Access Control	• Access rights must be assigned based on clearly defined roles and responsibilities within the organization. • Access rights, including those of privileged users, must be reviewed regularly (e.g., quarterly or bi-annually) .	• ISO/IEC 27001 (A.9.1, A.9.2): • NIST CSF (PR.AC-1, PR.AC-4):

Collaboration and Knowledge Sharing	Collaboration	• Encourage internal collaboration between departments (IT, cybersecurity, compliance). • Collaborate with suppliers and partners to share cybersecurity practices. • Establish formal relationships with law enforcement agencies, national cybersecurity emergency response teams (CERTs), and relevant financial regulatory bodies to coordinate responses to significant cybersecurity incidents.	• FFIEC Cybersecurity Assessment Tool: Domain 5 • ISO/IEC 27001: A.15.1.1 • ISO/IEC 27001: A.16.1.4 • NIST CSF: RS.CO-2
	Knowledge Sharing	• Participate in industry-level information-sharing initiatives. • Benchmark cybersecurity practices with peers.	• FFIEC Cybersecurity Assessment Tool: Domain 3 • NIST SP 800-181

The cybersecurity assessment tool proposed in this research is not only a response to existing challenges but also a strategic framework for enhancing the long-term security of Ethiopia's fintech sector. Implementing this tool will provide several benefits to both fintech companies and regulators, including improved protection of sensitive data, better compliance with national and international standards, and enhanced risk management capabilities:

- Enhanced Security Posture: By aligning with international standards and focusing on governance, competency, and resilience, organizations will be better equipped to safeguard their operations against cyberattacks.
- Risk Management: A structured approach to identifying, mitigating, and responding to risks will reduce exposure to cyber threats and enhance incident response.
- Regulatory Compliance: The tool supports fintech companies in meeting both national and international regulatory requirements, making them more competitive in the global market.
- Capacity Building: By promoting ongoing education and skill development, the tool contributes to building a cybersecurity-skilled workforce in Ethiopia.

4.5 Conclusion

This thesis underscore the critical importance of governance, competency, and resilience in achieving cybersecurity readiness within Ethiopia's fintech sector. By thoroughly evaluating the current cybersecurity practices, identifying gaps, and proposing practical solutions, the study provided a comprehensive assessment of the sector's capacity to address cybersecurity challenges.

The analysis of the four variables revealed significant gaps in cybersecurity readiness at both regulatory and company levels. These gaps pose notable risks to the integrity and security of the Ethiopian fintech ecosystem. The findings highlight the urgent need for targeted interventions to close these gaps, ensuring that both regulatory bodies and fintech companies are better equipped to manage emerging cyber threats.

To overcome these challenges, the study proposed the development of a cybersecurity assessment tool designed to evaluate organizational readiness. This tool offers an important resource for companies to benchmark their cybersecurity practices and identify areas that require improvement. Furthermore, the study recommends that the fintech industry prioritize efforts to enhance their cybersecurity capabilities, aligning with global best practices to raise their overall security posture.

The study also emphasizes the need for continuous improvement in cybersecurity practices across the fintech sector. By adopting the proposed assessment tool and focusing on strengthening governance, competency, and resilience, Ethiopian fintech companies can significantly improve their cybersecurity readiness and better protect themselves against the evolving landscape of cyber threats.

4.6 Validation

The purpose of the validation process is to evaluate the effectiveness of the proposed cybersecurity assessment tool within Ethiopia's fintech sector. The focus is to ensure that the tool effectively addresses identified vulnerabilities and fills the gaps revealed during the research. The tool has been specifically tailored to fit the unique cybersecurity challenges faced by Ethiopia's fintech ecosystem.

To validate the tool, experts from fintech companies and regulatory bodies were selected, alongside cybersecurity professionals from other sectors to gain comprehensive feedback. These experts reviewed the tool to assess its relevance to fintech operations and its broader applicability within the Ethiopian space. The validation process emphasized the tool's alignment with established international standards such as NIST, ISO, and FFIEC, ensuring that it adheres to global cybersecurity practices while addressing local needs.

The experts applied established evaluation methods, concentrating on several key areas of the tool:

- Its overall relevance and ease of use,
- The clarity of the requirements,
- Flexibility in adjusting to various operational contexts,, and
- The tool's adaptability to companies of different sizes, experiences, and financial capacities, ensuring its effectiveness across the industry.

Following the expert review, feedback was collected, and recommendations were made to refine the tool for better applicability across different scenarios. All feedback was propoerly considered and incorporated into the final tool design. The cybersecurity requirements were simplified and clarified to ensure that companies of all sizes and capacities can easily implement the tool, regardless of their specific operational contexts.

All comments and recommendations from the experts were carefully considered and integrated into the final version of the tool. The requirements were revised to make them simpler, more concise, and easier to understand, ensuring that companies of all sizes and capabilities can adopt the tool effectively, regardless of their specific circumstances.

The validation process confirmed that the cybersecurity assessment tool offers practical guidance for stakeholder communication, support companies to prioritizing cybersecurity threats, and assists in evaluating their overall security readiness. Experts highlighted the need for continual updates to the tool to keep pace with evolving cyber threats and regulatory demands, ensuring its long-term effectiveness.

In conclusion, the validation process demonstrated that the proposed cybersecurity assessment tool effectively addresses the research findings and industry challenges identified in this study. It offers fintech companies a practical solution to enhance their security measures, safeguard their customers,

reduce cybersecurity risks, and most importantly, establish a foundation for building a cybersecurity-aware fintech community and culture across the industry. With expert input integrated into the tool, it is now better suited to meet the specific needs of Ethiopia's fintech sector.

5 Limitation and Future Work

5.1 Introduction

Like any research, this study on the cybersecurity readiness of Ethiopia's fintech sector encountered several limitations that impacted its scope and findings. Understanding these limitations is important for interpreting the results and for providing direction for future research. Despite the effort to explore cybersecurity practices, resilience, and governance within the sector, certain challenges such as limited data access, stakeholder participation, and the early development stage of Ethiopia's fintech industry influenced the depth of the analysis.

The Limitations section outlines the key constraints faced during the study, including response bias, access to relevant stakeholders, and the absence of standardized cybersecurity practices in the fintech space. Recognizing these issues allows future researchers to take steps toward overcoming these challenges in their own work.

Looking ahead, the Future Work section proposes ways to build on this study's findings by addressing gaps and improving research methodologies. Recommendations for enhancing stakeholder engagement, increasing awareness about cybersecurity, and conducting more comprehensive data collection efforts are highlighted. Further exploration of the cybersecurity skills gap and the continuous development of assessment tools that adapt to emerging cyber threats are key areas where future research can contribute.

This section not only reflects on the limitations of the study but also sets the stage for advancing cybersecurity readiness in Ethiopia's fintech sector, providing a pathway for ongoing improvement in safeguarding the industry.

5.2 Limitation

As this research progressed, several unexpected challenges arose, which ultimately affected the study's results. Recognizing these limitations was important for maintaining transparency and guiding future research in this area. The difficulties encountered were related to the rapidly changing fintech industry in Ethiopia, the research methods used, and the general lack of awareness about cybersecurity readiness across the sector.

One major challenge was response bias, where some participants may have given subjective or inaccurate answers, affecting the quality of the data. To minimize this, randomization techniques were applied, and participants' knowledge was checked before collecting data. Responses that appeared biased were excluded from the final analysis. Despite these efforts, the risk of bias may still have influenced the findings, highlighting the need for ongoing improvements to ensure data accuracy in future studies.

Another limitation was the difficulty in accessing relevant data and getting participation owner and in full responsibility from stakeholders. Engaging with fintech companies, regulatory bodies, and other important groups was a challenging process, which restricted the amount of data collected and may have impacted the depth of the analysis.

On the other hand, the early stage of Ethiopia's fintech industry posed further challenges. Both regulatory bodies and companies often lacked familiarity with standardized cybersecurity practices, which limited the quality of responses. This lack of common understanding made it harder to gather deep and meaningful insights.

In the future, research should focus on overcoming these limitations by improving stakeholder involvement and increasing awareness within the industry. Better data collection and stronger engagement with stakeholders would lead to deeper insights into the cybersecurity readiness of Ethiopia's fintech sector, allowing for more accurate and useful findings.

5.3 Future Work

This research has laid the groundwork for further investigations within the fintech domain by identifying gaps and suggesting areas for future exploration. Several themes emerging from the study's findings and

demographic data present opportunities for deeper inquiry.

Gender Distribution in Cybersecurity and Resilience:

This study highlights the potential influence of gender on cybersecurity outcomes within fintech organizations. Further research could explore how gender diversity impacts cybersecurity readiness, with particular attention to the roles of women and men in cybersecurity. This inquiry could provide valuable insights for fintech companies, particularly in terms of team composition and hiring practices, and may reveal how a more balanced representation could enhance organizational security.

Age and Cybersecurity Readiness:

The relationship between age and cybersecurity readiness is another area that warrants closer examination. This research suggests that age may influence an individual's ability to recognize and address cybersecurity threats. Future studies could investigate whether younger professionals are more adept at handling emerging threats, while more experienced professionals might contribute through strategic planning and foresight. Understanding these dynamics could inform workforce development and cybersecurity training programs.

Cultural, Historical, and Psychological Factors in Cybersecurity:

Exploring cybersecurity readiness within the context of cultural and behavioral norms specific to Ethiopia offers a promising avenue for future research. Understanding how local attitudes toward risk, regulatory compliance, and trust in technology influence cybersecurity behaviors could provide critical insights for the Ethiopian fintech industry. Further investigation into the psychological and cultural factors that shape cybersecurity practices would enhance readiness and inform more effective policies.

Resilience, Development, and Risk Mitigation:

This study emphasizes the importance of organizational resilience in mitigating cybersecurity risks. Future research could focus on developing resilience frameworks specific to fintech organizations and examine case studies of companies that have successfully implemented strategies to reduce risk. In particular, examining how partnerships and risk management practices contribute to resilience in developing economies could offer practical insights for other emerging markets.

Technology Adoption and Cybersecurity Skills Gap

A deeper exploration of the cybersecurity skills gap is essential, particularly regarding the technological proficiency of fintech professionals. Future research could evaluate the effectiveness of existing training programs and the role of education in bridging this gap. Such efforts would help ensure the workforce is well-equipped to handle the evolving cybersecurity challenges within the fintech industry.

Addressing these areas will allow future research to build on the findings of this study, further contributing to the development of a strong cybersecurity culture within companies and the broader fintech sector.

References

[1] UN, "A DIGITAL FUTURE FOR ALL? THE IMPACT OF DIGITAL TECHNOLOGIES," 2020. Accessed: Nov. 11, 2023.

[2] S. Kumail Abbas Rizvi, B. Naqvi, and F. Tanveer, "Is Pakistan Ready to Embrace Fintech Innovation?," THE LAHORE JOURNAL OF ECONOMICS, vol. 23, no. 2, pp. 151–182, Dec. 2018, doi: 10.35536/lje.2018.v23.i2.a6.

[3] www.privacysolved.com, "Cybersecurity And Cyber Resilience In The FinTech Sector," DataGuidance.

[4] World Economic Forum, "The Global COVID19 Fintech Market Impact and Industry Resilience Study with the support of," 2022. Accessed: Nov. 11, 2023. [Online]. Available: https://es.weforum.org/publications/

[5] W. B. W. E. F. CCAF, "The Global COVID-19 Fintech Market Impact and Industry Resilience Study with the support of," 2019.

[6] T. Asfaw, G. Advisor, and A. Mulatu, "Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia Addis Ababa, Ethiopia," 2018.

[7] N. S. Iheanacho, "LEVERAGING FINANCIAL TECHNOLOGY: A COMPARATIVE ANALYSIS OF THE LEGAL READINESS OF NIGERIA FOR FINTECH DISRUPTION VIS-A-VIS OTHER JURISDICTIONS."

[8] Phoram Mehta and Steven Chan, "FinTech Cybersecurity: An ASEAN Outlook." [Online]. Available: https://www.ibm.com/sg-en/security/data-breach

[9] "UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector 2 nd Edition," 2011. [Online]. Available: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[10] Jason Mitchell, "Africa faces huge cybercrime threat as the pace of digitalisation increases," https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation/?cf-view.

[11] A. Bouveret, "WP/18/143 Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," 2018.

[12] O. Gulyas and G. Kiss, "Impact of cyber-Attacks on the financial institutions," in Procedia Computer Science, Elsevier B.V., 2023, pp. 84–90. doi: 10.1016/j.procs.2023.01.267.

[13] L. R. Paul and L. Sadath, "A systematic analysis on fintech and its applications," in Proceedings of International Conference on Innovative Practices in Technology and Management, ICIPTM 2021, Institute of Electrical and Electronics Engineers Inc., Feb. 2021, pp. 131–136. doi: 10.1109/ICIPTM52218.2021.9388371.

[14] UN, "Systems of Cyber Resilience: Secure and Trusted FinTech Shaping the Future of Cybersecurity and Digital Trust Shaping the Future of Financial and Monetary Systems," 2020. [Online]. Available: www.weforum.org

[15] T. Thimot, "Cyber Threats to the Fintech Industry a Growing Concern," https://fintechmagazine.com/financial-services-finserv/cyber-threats-fintech-industry-growing-concern.

[16] F. Moses and N. Ogbuefi, "Cybersecurity in the Age of FinTech and Digital Business," 2019. [Online]. Available: https://ssrn.com/abstract=3606866

[17] Ademola Adeyoju, "CYBERCRIME AND CYBERSECURITY: FINTECH'S GREATEST CHALLENGES," 2019. [Online]. Available: https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber

[18] P. Musuva, "Cybersecurity Risks and National Policy Implications-East African Experiences Case 2 The Research Team Sponsor The Global Business School Network (GBSN) Funder The SWIFT Institute Report Date," 2021.

[19] H. M. K. Al Duhaidahawi, J. Zhang, M. S. Abdulreda, M. Sebai, and S. Harjan, "Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks," International Journal of Research in Business and Social Science (2147- 4478), vol. 9, no. 6, pp. 123–133, Jan. 2021, doi: 10.20525/ijrbs.v9i6.914.

[20] S. Mehrban et al., "Towards secure FinTech: A survey, taxonomy, and open research challenges," IEEE Access, vol. 8, pp. 23391–23406, 2020, doi: 10.1109/ACCESS.2020.2970430.

[21] J. A. R. C. Jayalath and S. C. Premaratne, "Analysis of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies," International Journal of Research Publications, vol. 84, no. 1, Aug. 2021, doi: 10.47119/ijrp100841920212246.

[22] A. Ahmed Ali, "DIGITAL ETHIOPIA 2025A STRATEGY FOR ETHIOPIA INCLUSIVE PROSPERITY DIGITAL ETHIOPIA 2025A STRATEGY FOR ETHIOPIA INCLUSIVE PROSPERITY Prime Minister Federal Democratic Republic of Ethiopia DIGITAL ETHIOPIA 2025A STRATEGY FOR ETHIOPIA INCLUSIVE PROSPERITY," 2018.

[23] A. A. Moustafa, A. Bello, and A. Maurushat, "The Role of User Behaviour in Improving Cyber Security Management," Frontiers in Psychology, vol. 12. Frontiers Media S.A., Jun. 18, 2021. doi: 10.3389/fpsyg.2021.561011.

[24] W. Jerene and D. Sharma, "The adoption of financial technology in Ethiopia: a study of bank customers perspective," Journal of Banking and Financial Technology, vol. 4, no. 1, pp. 53–63, Apr. 2020, doi: 10.1007/s42786-020-00015-0.

[25] S. AlBenJasim, T. Dargahi, H. Takruri, and R. Al-Zaidi, "FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study," Journal of Computer Information Systems. Taylor and Francis Ltd., 2023. doi: 10.1080/08874417.2023.2251455.

[26] S. Baur-Yazbeck, J. Frickenstein, and D. Medine, "CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT Challenges and potential solutions for financial inclusion," 2019.

[27] S. B.-Y. Juliet Maina, "Digital Finance: Cybersecurity Requires Deeper Industry Collaboration," https://www.cgap.org/blog/digital-finance-cybersecurity-requires-deeper-industry-collaboration.

[28] S. Baur-Yazbeck, J. Frickenstein, and D. Medine, "CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT Challenges and potential solutions for financial inclusion," 2019.

[29] RODRIGO FERREIRA DA MATA CRISTÓVÃO "fintech-landscape-in-sub-saharan-africa—the-case-of-mozambique-how-can-a-peer-to-peer-lending-fintech-serve-mozambican-investors", 2021.

[30] G. Murillo Velazquez and B. A. Washington, "THE EFFECT OF NATIONAL CYBERSECURITY COMMITMENT ON FINANCIAL INCLUSION," 2023.

[31] Tornatzky LG, Fleischer M, Chakrabarti AK. Processes of Technological Innovation. 1990. Lexington books.

[32] Facilitating innovation in FinTech: a review and research agenda, Ahmad Alaassar1,2,3 · Anne-Laure Mention2,4,5,6 · Tor Helge Aas3

[33] R. M. Kaibiru, S. M. Karume, F. Kibas, and M. L. B. Onga'nyo, "Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education," Journal of Information Security, vol. 14, no. 02, pp. 136–151, 2023, doi: 10.4236/jis.2023.142009.

[34] Ayo Maxwell Alabi, Fuzzy Naomi Oguntoyinbo, Kehinde Mobolaji Abioye, Adesola Adepeju John-Ladega, Anwuli Nkemchor Obiki-Osafiele, and Chibuike Daraojimba, "RISK MANAGEMENT IN AFRICA'S FINANCIAL LANDSCAPE: A REVIEW," International Journal of Advanced Economics, vol. 5, no. 8, pp. 239–257, Oct. 2023, doi: 10.51594/ijae.v5i8.573.

[35] David Carnal, "5 ways cyberattacks can damage a company's reputation," https://www.anapaya.net/blog/5-ways-cyberattacks-can-damage-a-companys-reputation.

[36] A. Bouveret, "WP/18/143 Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," 2018.

[37] M. H. Uddin, M. H. Ali, and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," Risk Management, vol. 22, no. 4, pp. 239–309, Dec. 2020, doi: 10.1057/s41283-020-00063-2.

[38] L. B. Christensen, Burke. Johnson, and L. Anne. Turner, Research methods, design, and analysis.

[39] "NBE Financial Consumer Protection Directive 2020".

[40] FFIEC Cybersecurity Assessment Tool, May 2017

[41] https://www.ncsc.gov.uk/collection/cyber-assessment-framework

[42] https://swimlane.com/blog/top-cybersecurity-frameworks/

[43] The NIST Cybersecurity Framework (CSF) 2.0

[44] https://www.techtarget.com/searchsecurity/definition/NIST-Cybersecurity-Framework

[45] ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY, Sarah Kuzankah Ewuga1, Zainab Efe Egieya2, Adedolapo Omotosho3, & Abimbola Oluwatoyin Adegbite4

[46] Cybersecurity Capability Maturity Model, Version 2.1

[47] CIS Critical Security Controls Version 8 May, 2021

[48] Towards a Theoretical Foundation of IT Governance – The COBIT 5 case

[49] Framework for Improving Critical Infrastructure Cybersecurity, 2018 (Version 1.1)

[50] Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs) Maria Bada Computer Laboratory, University of Cambridge, Cambridge, UK, and Jason R.C. Nurse School of Computing, University of Kent, Canterbury, UK

[51] https://www.imf.org/en/Blogs/Articles/2022/04/13/blog041322-sm2022-gfsr-ch3

[52] https://www.hedgethink.com/the-role-of-ethiopia-in-shaping-the-fintech-future-of-africa/

[53] https://timeseriesreasoning.com/contents/f-test-for-regression-analysis/

[54] FINTECH, THE NEW ERA OF FINANCIAL SERVICES, Article · November 2017

[55] Understanding SaaS adoption: The moderating impact of the environment context Tiago Oliveiraa, Ricardo Martinsa , Saonee Sarkerb, Manoj Thomasc, Aleš Popoviča,d,∗

[56] Electronic Business Adoption by European Firms: A Cross-country Assessment of the Facilitators and Inhibitors

[57] Studying Users' Computer Security Behavior Using the Health Belief Model. Boon-Yuen Ng and Yunjie (Calvin) Xu

[58] Literature Review of Information Technology Adoption Models at Firm Level, Tiago Oliveira and Maria Fraga Martins

[59] The Technology–Organization–Environment Framework

[60] The processes of technological innovation. Lexington, MA: Lexington Books.Tornatzky, L. G., & Fleischer, M. (1990).

[61] Business Statistics, 4th Edition, By J. K. Sharma ·2014

[62] Montgomery, D. C. (2019). Design and Analysis of Experiments. Wiley.

[63] FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY Jennifer Callen-Naviglia, PNC Bank, dr.callennaviglia@gmail.com Jason James, Sullivan University, je-james@sullivan.edu

[64] Cybersecurity Regulation in Singapore's Financial Sector: Protecting FinTech 'Ants' in a Jungle Full of 'Elephants'

[65] https://psi.org.et/index.php/blog/266-ethiopia-s-digital-finance-sector-overcoming-challenges-and-driving-financial-inclusion#: :text=Several%20factors/20contribute%20to%20the,digital%20literacy%2C%20and%20

[66] Basel Committee on Banking Supervision, 2018, p. 11

[67] Financial Supervisors and RegTech: Four Roles and Four Challenges; Luca Enriques

[68] Financial Sector's Cybersecurity: A Regulatory Digest, 2017

[69] CREATING ENABLING FINTECH ECOSYSTEMS: THE ROLE OF REGULATORS

[70] https://www.insurance-canada.ca/2019/01/21/accenture-cyber-crime-cost-study/

[71] https://www.msspalert.com/news/accenture-cybercrime-findings

[72] FinTech and market structure in financial services: Market developments and potential financial stability implications

[73] FinTech in Sub-Saharan African Countries A Game Changer?

[74] Report on the Implementation of the Strategic Plan and activities of the Union, April 2019 – April 2020

[75] Global Cybersecurity Index 2020

[76] Cyber Risks and the Integrity of Digital Finance.(2021)

[77] "Fintech and Payments Regulation: Analytical Framework." IMF Working Papers, (2020).

[78] NICE Framework Components v1.0.0: Summary of Changes.

[79] Fisher, R. A. (1925). Statistical Methods for Research Workers.

A Appendix A: Invitation to Participate in Research Study

Dear Respondent,

You are kindly invited to participate in a research study conducted by Teklehymanot Meheret, a graduate student in the Cybersecurity, Cyber Governance, and Management program at Addis Ababa University (AAU), Addis Ababa Institute of Technology (AAiT). The purpose of this invitation is to engage professionals working as cybersecurity experts, leaders, and managers in a survey.

Your participation in this study is entirely voluntary, and you have the right to decline to answer any question at your discretion, without any penalties or consequences. Your cooperation in this research endeavor is highly valued and appreciated.

The main objective of the research questionnaire is to collect information regarding the cybersecurity readiness of the fintech ecosystem in the country. This will be achieved by assessing the individuals, companies, and regulatory bodies respectively. Your involvement and responses will significantly impact the research output and help understand the real challenges faced by the industry.

The information you provide in response to the questionnaire items will be used as part of the survey data required for this thesis to obtain reliable and relevant information for the study. All the information you provide will be kept strictly confidential and will be used solely for academic research purposes. Please answer each question carefully, as there are no right or wrong answers. If you are unsure about an answer, please respond with your best estimate.

Your participation, time, energy, and effort are highly valued and appreciated. If you have any further questions, you can reach me at the following addresses.

Sincerely,
Teklehymanot Meheret
Email: dvisor: Elefelious G. Belay (Ph.D)

Thank you for your consideration and support in advancing this important research endeavor.

B Appendix B: DEMOGRAPHIC INFORMATION

1. Gender
    a. Male
    b. Female
2. Age
    a. 20 - 30
    b. 31 - 40
    c. 41 - 50
    d. ¿ 50
3. How many years of experience do you have in cybersecurity?
    a. 1 - 3
    b. 4 - 10
    c. More than 10
4. What is your position?
    - _____

C Appendix C: Question For Regulator

Please choose one response 1: - Strongly Dis Agree, 2: - Disagree, 3: -Neutral, 4: - Agree 5: - Strongly Agree

Code	Question	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
GFRQ1	The country established a cybersecurity policy specifically tailored for the fintech sector?					
GFRQ2	The cybersecurity policy is regularly updated to address emerging cyber threats and evolving technologies?					
GFRQ3	The country has a mechanism for violations or non-compliance with the cybersecurity policy to be promptly identified and addressed through appropriate actions or penalties?					
GFRQ4	The country has guidelines and procedures in place for fintech companies to report any deviations or non-compliance with the security standards?					
GFRQ5	Compliance with cybersecurity policies and controls is regularly monitored and enforced within organizations?					
GFRQ6	The country has a comprehensive and well-defined regulatory framework specifically tailored for the fintech sector?					
GFRQ7	There are clear guidelines and processes in place for fintech companies to obtain necessary approvals, licenses, and certifications?					
GFRQ8	The regulatory authorities provide guidance and support to fintech companies in interpreting and implementing the recommendations from cybersecurity assessments?					
GFRQ9	The regulatory authority has made it mandatory for fintech companies to follow specific cybersecurity standards, frameworks, and best practices?					
GFRQ10	The data protection laws and regulations governing the collection, usage, and consent practices related to personal data within the fintech sector are comprehensive, with adequate measures/guidelines to ensure strict adherence by fintech companies?					
GFRQ11	The regulatory authority provides clear guidelines and best practices for emerging technologies (e.g., cloud computing, mobile payments, blockchain) that fintech companies can refer to while implementing security controls?					

GFRQ12	There is a standard and framework for identifying and classifying assets in the fintech sector to put in place appropriate controls and protection?					
GFRQ13	A secure software development life cycle standard and framework are in place to encourage companies to follow and incorporate in the development practice?					
GFRQ14	There is an effective system in place to regularly check, assess, and monitor that companies are properly following and complying with cybersecurity requirements?					
RFRQ15	Incident response plans and procedures are in place within the fintech ecosystem to effectively manage and mitigate the impact of cyber incidents?					
RFRQ16	There is an effective risk management framework and methodology to identify, assess, and mitigate cyber risks in the fintech sector?					
RFRQ17	There is a well-defined process for conducting regular cybersecurity audit assessments with appropriate guidance/oversight from the regulatory authority?					
RFRQ18	Companies are encouraged to conduct penetration testing and vulnerability assessments on their systems and applications to identify potential security weaknesses regularly?					
RFRQ19	There is a national framework for fintech companies to have well-documented and tested incident response and business continuity plans to effectively manage and recover from cyber incidents?					
RFRQ20	Security measures such as multi-factor authentication, encryption, and tokenization are implemented by fintech companies to protect customer data and transactions?					
RFRQ21	There is effective leveraging of threat intelligence and information-sharing platforms to stay informed about the latest cybersecurity threats and attack vectors?					
CFRQ22	Legal/regulatory frameworks require fintech companies to provide comprehensive cybersecurity awareness and training programs?					
CFRQ23	A national cybersecurity awareness and training program is in place to promote a cybersecurity culture in the fintech sectors?					

CFRQ24	The fintech sector has established dedicated cybersecurity teams or personnel responsible for implementing and maintaining cybersecurity?					
CFRQ25	The current cybersecurity workforce possesses specialized skills and expertise required to support the cybersecurity needs of the fintech sector?					
CFRQ26	There are effective initiatives/policies in place to cultivate a skilled cybersecurity workforce that can meet the industry's present and future talent needs?					
CFRQ27	Sufficient financial, technical, and human resources are allocated specifically dedicated to cybersecurity initiatives within the fintech sector to effectively implement and enforce cybersecurity policies and programs?					
CFRQ28	There is a platform for sharing, collaboration, and coordination with relevant stakeholders in cybercrime, vulnerability, cybersecurity incidents, and threats in the fintech ecosystem?					
CFRQ29	The government provides incentives, grants, or funding opportunities to encourage cybersecurity research, innovation, and skill development in the private sector and academic institutions?					
PFRQ30	Cybercrime has become a major concern and a top priority for financial institutions and regulators in the country?					

D Appendix D: Question For FinTech Company

Please choose one response 1: - Strongly Dis Agree, 2: - Disagree, 3: -Neutral, 4: - Agree 5: - Strongly Agree

Code	**Question**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
GFCQ1	The company has a well-defined cybersecurity policy which is regularly evaluated and adopts industry-recommended cybersecurity frameworks and standards (e.g., NIST, ISO, CIS)?					
GFCQ2	The company has a data protection and privacy policy that aligns with the country's regulations for the collection, storage, and sharing of customer data?					
GFCQ3	The company's policies and procedures are regularly reviewed and updated to align with changes in legal and regulatory requirements?					
GFCQ4	The company has a risk management framework and methodology to assess, identify and mitigate cyber risks?					

Code	Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
GFCQ5	The company has guidelines for managing third-party systems and data access?					
GFCQ6	The company has a process to monitor and ensure compliance with relevant industry standards, regulations, and legal requirements specific to the fintech sector?					
GFCQ7	The company has a comprehensive data classification policy in place to guide the proper handling, storage, and protection of sensitive information and customer data?					
GFCQ8	The company has a well-defined access control and privileges access management policy to prevent unauthorized access?					
RFCQ9	The company has a process for violations or non-compliance with the cybersecurity policy addressed through appropriate actions or penalties?					
RFCQ10	The company's cybersecurity practices are regularly audited and validated (e.g., annually, bi-annually) through a comprehensive process?					
RFCQ11	The company has well-established processes for reporting, investigating, and addressing potential data breaches and violations?					
RFCQ12	The company has business continuity plans to guarantee seamless operations in case of a security disaster?					
RFCQ13	The company has a vulnerability management program that includes regular scanning, patching, and remediation of identified vulnerabilities?					
RFCQ14	The company has a well-defined and regularly tested incident response plan to effectively manage and recover from cybersecurity incidents?					
RFCQ15	The company's cloud services have adequate security controls and measures in place to ensure the protection of data and systems in the cloud environment?					
CFCQ16	The company has a comprehensive security awareness and training program that covers various aspects of cybersecurity for employees, contractors, and third-party vendors?					
CFCQ17	The company has established a process to identify skills gaps in cybersecurity, with a focus on recruiting, retaining talent and expertise as a top priority?					

Code	Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
CFCQ18	The company established dedicated cybersecurity teams or personnel responsible for implementing and maintaining cybersecurity?					
CFCQ19	The company utilizes a dedicated platform or system for sharing, collaborating, and coordinating with relevant stakeholders in the fintech ecosystem regarding cybercrime, vulnerabilities, incidents, and threats?					
CFCQ20	The company understands the commitment for cybersecurity as a strategic priority, including the allocation of an adequate budget to maintain its market positioning and competitiveness?					
CFCQ21	The company has effective communication channels for disseminating cybersecurity updates and guidelines to employees?					
CFCQ22	The company effectively monitors and controls employee behaviors related to the processing of sensitive data and information-sharing practices to mitigate potential risks?					
CFCQ23	The company has a cybersecurity culture program for integrating cybersecurity training into the onboarding process for new employees?					
PFCQ24	The company demonstrates a comprehensive understanding of the legal and regulatory landscape in the Ethiopian fintech industry, and actively engages with regulatory authorities?					
PFCQ25	The company collaborates and shares cybersecurity knowledge with industry peers and organizations?					
PFCQ26	The company keeps an effort to stay updated about emerging cybersecurity threats and adhering to best practices specific to the fintech industry?					
PFCQ27	The company follows secure coding practices and incorporates security considerations throughout the software development life cycle in-house software and application development practice?					