[ABAYOMI T. OLUTIMEHIN]

[Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in Banking Sector and Its Applicability to Decentralized Finance (DeFi)]

Submitted as part of the requirements for the award of the
MSc in Information Security
at the Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature: **ABAYOMI OLUTIMEHIN** Date: 27/08/2024

Contents

Glossary and Definitions

Terms	Definition
Digital Assets	Any asset that is purely digital, or is a digital representation of a physical asset. https://csrc.nist.gov/glossary/term/digital_asset [1]
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." https://csrc.nist.gov/glossary/term/confidentiality[1]
Integrity	The term 'integrity' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. https://csrc.nist.gov/glossary/term/integrity[1]
Availability	Ensuring timely and reliable access to and use of information. https://csrc.nist.gov/glossary/term/availability[1]
Risk	is a measure of the extent to which an entity is threatened by a potential circumstance or event
Threats	is any circumstance or event with the potential to adversely impact organizational operations and assets
Vulnerability	is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
TVL	Total Value Locked (TVL) is a metric used to measure the total value of digital assets that are locked or staked in a particular decentralized finance (DeFi) platform or decentralized application (dApp). (Reference - Total Value Locked (TVL) - Techopedia) [2]
IMF	Internation Monetary Fund - A global organisation that monitors economies, provides financial aid, and conducts research

Keywords: Financial Sector, Decentralized Finance (DeFi), Traditional Banking, Blockchain, Security Standards, Regulatory Frameworks, Cybersecurity Frameworks, FinTech, RegTech, Financial Regulation, Digital asset.

Executive Summary

The innovations that brought about services that had previously been completed face-to-face and with pen and paper which is now completed virtually and digitally also opened up a whole new vector and opportunities for corresponding levels of threats and crimes. The digitisation of the financial landscape has given rise to a significant transformation in the banking sector and along with it comes an upsurge in cyber-enabled threats. These innovations have necessitated the institution of corresponding strategies to plug every attack surface and vector that has been created as far as technology is concerned, examples of such strategies are the promulgation of cybersecurity laws like the EU General Data Protection Regulation (GDPR) or the UK Data Protection Act (DPA) 2018, prescriptive regulatory frameworks such as PCI-DSS and standards (best practices guidelines) e.g. NIST and ISO2700, all collectively referred to as cybersecurity frameworks are designed to fortify the sector against security breaches, but majority of these cybersecurity frameworks mostly apply within traditional banking and financial sector, these new technological enabled changes and concepts e.g. Blockchain, Crypto Assets, etc., which are currently indeterminate have become easy areas of attack judging by share scale and frequency of the attacks and the cost associated with such attacks.

These widespread impacts of technological advancements have brought about significant transformations in various aspects of society, notable among them is the categorisation of the banking and financial industries as Critical National Infrastructure (CNI) in 2007. This is rightly so, the implications of potential cybersecurity attacks in this sector are profound, with the potential to disrupt the economic fabric of a nation as was the case when Russia's attack on Ukraine's government and Banking sector in 2022, the German bank hit in 2021[1].

In response to this new form of onslaught, many governments across the world have responded by making executive orders for targeted actions for their jurisdiction, an example was the US Executive Order 13636 signed by President Obama in 2013 which led to the creation of NIST CSF in 2014, the European Union has also taken both proactive and reactive approaches at different times (depending on the circumstances and criticality of the threats) by creating several regulations and directives for member states such as NIS2 and DORA, alongside antecedent regulations, GDPR to safeguard data—a highly valued asset in the face of cyber threats. National governments also have different governmental regulatory organisations that task with regulating the financial sector and preparing for this acts of war, cyberwarfare, e.g. Financial Conducts Authority (FCA), Bank of England in the UK.

Technological advancements such as Artificial Intelligence AI, Machine Learning ML, Blockchain, Cryptocurrency, Robotics, Internet of Things IoT, all brings both advantages, new opportunities, unique challenges and inherent risks. The Financial sector has been a leader in technology and innovation with the aim to protect valuable data from cyber criminals and enhance customer banking experiences, thereby driving business engagement to increase their market share and profitability. This dual approach has led to the modernization of banking infrastructure and also opened up avenues for cybercriminals [2].

Through a comprehensive literature review, this study evaluates the efficacy of current cybersecurity frameworks in mitigating cyberattacks within the traditional banking sector, as well as their relevance to the rapidly growing DeFi sector. The review also aims to highlight existing gaps in available research and propose areas for future research.

Chapter 1: Introduction

1.1. Motivation for the Research Topic

I am an Information Security Specialist and Internal Security Assessor with over eight years of hands-on experience within the UK Financial Services industry. My primary responsibility within the Governance, Risk and Compliance (GRC) functions of the bank includes assessing and ensuring that the banks security program is effective and fit for purpose. I focus on ensuring that adequate security through targeted risk assessments, compliance with adopted security standards, mandatory regulatory frameworks, and other security strategic programs are in place to deliver robust security that improves the bank's security profile while keeping the bank resilient against threats and ensuring our measures effectively detect and prevent potential risks.

I propose to study the applicability of time-tested cybersecurity practices, particularly cybersecurity frameworks as a tool that had been used in combating cyber threats and cyberattacks in the traditional banking sector to the new and emerging field of decentralized finance (DeFi). The banking sector has long been a prime target for cyber threats, with attacks evolving along with technological advancements. Historical trends show a shift from insider threats [3] to more sophisticated external attacks, including malware and advanced persistent threats [4]. The sector faces disproportionate risks due to its critical economic role [3]; these attacks extend beyond direct financial losses, it affect customer trust, banks' reputation and overall economic stability [5]. In response to the various threats, the Financial sector has a range of safeguards and countermeasures including various technical, non-technical, and organisational controls to combat the threats and adhere to legal and regulatory frameworks [6]. The provision of financial services through a combination of infrastructure, markets, technology, methods, and applications in a decentralized manner is referred to as Decentralized Finance (DeFi). It is the provision of financial services through multiple participants, intermediaries, and end-users spread across multiple jurisdictions, with technology facilitating and often enabling their interactions [7]. Decentralized Finance (DeFi) represents a cutting-edge technology, in the industry that integrates decentralization, blockchain technology distributed ledger technology, smart contracts, direct transactions, without intermediaries and open banking [8], [9]. While the term "decentralized" may have varying interpretations it commonly denotes services offered by a group of parties including intermediaries and end users spread across different locations worldwide [10].

DeFi has gained considerable prominence in recent years, it emerged with the promise that it is able to disrupt conventional financial systems, built on blockchain technology and

smart contracts, operationally it facilitates direct peer-to-peer transactions and eliminates the requirement for intermediaries. While some financial institutions see it as an opportunity and are embracing it, others are still sceptical about it and currently stay away from it. The same can be said of countries, the acceptance of DeFi by national governments varies across the globe, some outrightly ban DeFi, while others embrace it. From my initial research, it is quite clear that DeFi has suffered many cyberattacks: on the decentralised technologies and protocols front (the backbone) and finance implementations front.

Some of the DeFi-associated Risks which has been broadly categorised as technical, operational, legal and regulatory risks [11] includes execution risks in smart contracts, legal liability risks, data theft risks, interconnectedness risks, external data risks, and the increased propensity for illicit activity with Decentralized Applications (DApps) [12]. While not all these risks are cybersecurity-related, this project will focus on specific cyber-related ones as I attempt to compare these risks in DeFi to similar risks in traditional banking, analyse how these risks are currently mitigated, and evaluate whether this knowledge can be applied to DeFi with the hope of making valuable contributions to the emerging field.

This study underscores several critical research gaps:

a) There is a scarcity of comparative research that examines the efficacy of cybersecurity frameworks between traditional banking and DeFi.
b) There is an insufficiency of research that focuses on the rapid development of cyber threats, particularly within the DeFi context.
c) There is an insufficient works exploring the potential adaptation of traditional banking security standards to DeFi's unique environment.
d) There is an urgent need for empirical evidence that assesses the actual effectiveness of these frameworks against cyber-attacks.

In response, this study seeks to address or fill some of these gaps through:

a) An analysis to ascertain the relative effectiveness of security frameworks across both the Banking and DeFi sectors.
b) An investigation into how traditional Banking security standards might be repurposed or expanded to incorporate DeFi security challenges.
c) Gathering and analysing data to corroborate the real-world experiences of professional on the efficacy of these security frameworks in countering cyber risks.

1.2. Statement of Objectives

This dissertation aims to evaluate the role of Cybersecurity Frameworks in mitigating cyberattacks within the traditional banking and financial sector and explore their potential

applicability to Decentralized Finance (DeFi). I will attempt to achieve the following objectives:

1. Ascertain the extent to which existing Cybersecurity Frameworks has had an influence in the Security landscape of Banks, focusing on key aspects of the widely used frameworks and impact on cyber resilience within the sector.
2. Explore the potential applicability of insights gained from the banking sector's experience with Cybersecurity Frameworks in the burgeoning field of Decentralised Finance (DeFi).
3. Given DeFi's unique architectural and operational characteristics, this study investigates the feasibility and implications of adapting and implementing similar cybersecurity Frameworks within this innovative financial domain.
4. Provide a comprehensive understanding of DeFi's regulatory needs and challenges, offering recommendations for stakeholders to enhance security and resilience against cyber threats.

1.3. Structure of the Report

This report has been carefully crafted to help readers smoothly navigate through its chapters ensuring a transition, from one section to the next. The goal is for the report to present a flow where each new chapter builds upon the one in a logical manner with each preceding chapter laying the groundwork for what follows. The introduction gives an in-depth look at the matter while the conclusion highlights discoveries and provides suggestions, for future studies.

Chapter 1 introduces the project, clearly stating the aim and objectives, motivation for the research, and methodologies used.

In Chapter 2, I will examine the usage of Cybersecurity Frameworks in the conventional Banking Sector, identify the most frequent and severe cyber threats within the sector, and evaluate the ability of Cybersecurity frameworks to mitigate such cyberattacks. Additionally, the chapter will explore the current state of security hygiene within the DeFi ecosystem, identify the most common cyberattacks in that ecosystem, and compare the similarities and differences between DeFi and traditional Banking cyber threats. Finally, the chapter will assess the potential of Cybersecurity frameworks in mitigating these cyber threats and analyse the boundaries of these frameworks in tackling emerging cyber threats, emphasising the need for continuous adaptation to stay ahead of the changing threat landscape.

In **Chapter 3,** I describes the type of the research that was conducted and the reasons why I have gone with the methodological approach selected. I also described the challenges I encountered and the ethical considerations that guided me in the decision-making process.

Additionally, I discussed how the data was cleaned, and the steps taken to mitigate any potential biases that may have arisen during the research. Moreover, the paper underscores the significance of recognising the potential limitations of the selected research method and addressing them in the analysis to guarantee the credibility and dependability of the findings.

Chapter 4 presents the results of the research conducted on the research topic. The study's results are presented clearly and concisely in this chapter, allowing for easy understanding and interpretation. The clarity and precision of the research findings presented in this chapter make it straightforward for readers to comprehend and evaluate the results effectively.

Chapter 5, the final chapter of this research study, concludes by summarising the main findings and highlighting the significant contributions made to the field. It reflects on the broader implications of the research and emphasizes the practical recommendations for future research that build upon the findings of this study and expand upon the existing knowledge of the subject. The study's results offer new perspectives on the subject matter and valuable insights for further research.

Chapter 2: Overview of Cybersecurity Frameworks in the Banking Sector

The objective of this dissertation which is in two fold seeks to understand the effectiveness of cybersecurity frameworks in traditional banking and financial sector. Cybersecurity frameworks are a collection of risk-based governance tools that are designed to provide a system of repeatable practices capable of guiding an organisation's cybersecurity strategy and security programmes to ensure stability and resilience against cyberattacks [13]. The two broad categories of Cybersecurity Frameworks are Security Standards which provide a set of controls that forms baseline guidance and non-mandatory safeguards /controls /countermeasures for establishing, implementing, maintaining, and continually improving information security management systems within an organisation; they help provide structure and consistency to organisations for the Security Strategy and program. Examples of such Standards include the ISO27001/2 [14] and NIST CSF and SP (Special Publication) series [15]. Implementing these standards enables organisations to protect their information systems and infrastructures. It also enables them to be able to demonstrate their commitment to maintaining high levels of security and safeguarding their business-sensitive information to their stakeholders and interested parties, in some situations, inability to demonstrate this level of compliance may result in loss of business e.g. the US government will not do business with any organisation that is not using the NIST frameworks. Establishing and maintaining a robust information security management system that aligns with industry best practices will give them the confidence of compliance with regulatory requirements and assurances for cybersecurity resilience (the ability to bounce back in the event of an attack).

The second category of cybersecurity frameworks are legal and regulatory frameworks. They are mandatory for specific or participating industries and organisations to follow, lack of compliance can result in loss of business, regulatory fines and other financial consequences. The requirement to comply maybe by choice or by legal decree in the area of business or jurisdiction. For example, any organisation in the UK that processes personal data must comply with UK DPA. An organisation may also choose to outsource the functions of their business that requires them to comply with legal or regulatory standards to other businesses to manage for them. e.g. a retail business may choose to use a payment service provider to process payment for them rather than doing it themselves which may bring them in scope for PCI-DSS. Examples of these regulatory frameworks include the PCI-DSS [16] and the Health Insurance Portability and Accountability Act (HIPAA) [17], both of which aim to protect sensitive information and ensure compliance with industry standards. Other examples include the General Data Protection Regulation (GDPR) [18] or its UK equivalent UK Data Protection Act

2018 [19], both of which aim to safeguard personal data and enforce strict data protection measures; and the Sarbanes-Oxley Act (SOX) [20], which is designed to protect sensitive information and ensure compliance with industry standards.

2.1. Cybersecurity in the Financial and Banking Sector

2.1.1. Overview of Cybersecurity Threats

The banking industry has historically been a top priority for criminals generally even before cyber-enabled crime emerged. The estimated cost of cybercrime in this sector is expected to reach 9.5 trillion USD by 2024 [10]. This should come as no surprise, given the critical-sensitive position that the financial services sector occupies in any nation, in the face of constantly evolving cyber threats, financial service organisations control assets that are desirable to cyber criminals, they have money and assets that can be turned into money in the dark market (e.g. sensitive information about customers and their transactions) making them preferable targets for cybercriminals of different categories including state-sponsored actors, cyberterrorist, hackers, identity thieves etc.

Although historical trends show a shift from insider threats [3] to more sophisticated external attacks, including malware and advanced persistent threats.[4]. The most common threats facing the financial sector are Malware, Phishing, and Ransomware attacks [21], [22]. Two (2) of the 6 biggest threats to financial services in 2024 have been identified as Phishing and Ransomware attacks, the other four are SQL injections, DDoS Attacks, Supply Chain attacks, and Bank Drops [23]. The sector faces disproportionate risks due to its critical role in the economy. [6] The impact of these attacks extends beyond direct financial losses, affecting customer trust and overall economic stability. [24] Various technical, non-technical, and organisational countermeasures and strategies for adhering to legal and regulatory frameworks are deployed sector-wide to combat these threats. [6]

Recent cyberattacks in the financial sector have become increasingly sophisticated and frequent, particularly during the COVID-19 pandemic [25]. Emerging technologies such as AI have added another level of complication, with AI being a useful tool both for the attacker to launch sophisticated attacks and the attack employing the same level of sophistication to defend itself against attacks [26]. As a prime target, the banking sector faces complex threats due to its critical economic role [6]. To combat these multidimensional threats to financial institutions, a proposed novel approach is the adopting advanced cybersecurity measures and advanced analytic, strategic approaches for fraud detection techniques such as "Robotic Process Automation (RPA)" [27] Frameworks for estimating potential losses due to cyber risks have been developed [28], and Bayesian Attack Network modelling is being used to mitigate

malware-based attacks [21]. To tackle the multifaceted challenges that financial institutions face, a new approach has been proposed, which involves implementing advanced cybersecurity measures and utilizing sophisticated analytic and strategic approaches for fraud detection, such as "Robotic Process Automation (RPA)" [23]. In addition, frameworks have been developed to estimate potential losses resulting from cyber risks [24], and Bayesian Attack Network modelling is being employed to mitigate malware-based attacks [21].

2.1.2. Impact of Cyber-attacks

The services and products that the financial services provided have been greatly transformed and enhanced by technological advancements; this inevitably has resulted in a larger attack surface compared to pre-technology-enabled products and services. A lot of research has gone into reasons why people commit crimes; the popular reasons are to maximise financial gain, for power and control, or to inflict the most impact as such, they choose their targets accordingly; hence, one targeted attack on financial services can help cyber criminals to achieve some or all of this goals. Attacks on banks have since moved on from local operations in the era of daredevils walking through banking halls with guns; they are now facing a different form of attack that is more sophisticated and far-reaching, cyber-enabled crimes [29]. Cyber-enabled attacks are a significant threat to the financial sector; with the help of technology, the attack vectors have not only increased, but the impact of the attacks can be disruptive, severe, costly, far-reaching, and sometimes cause severe economic consequences, some of the impacts both to the bank and its customers are customer data breaches, organisation reputational damage, financial fraud and legal and regulatory fines and cost [30]. An example was the DDoS attack on a German IT provider that impacted the country's 800 cooperative banks in 2021 [31]. The attacks have increased in frequency, severity and impact over the years, a database of cyber incidents that target financial institutions records over 200 attacks worldwide between 2007 and 2021 [32]. The financial impact is substantial, with billions lost annually to cybercrime [26]; in May of 2024, the International Monetary Fund (IMF), warning about the threat of cyberattacks to global financial stability, reported that the financial sector had suffered over 20,000 cyberattacks resulting in losses of $12 Billion in the last 20 years [33]. Research on the top threats facing the Financial sector in 2024 reveals a lack of consensus; it is, however, not shocking that virtually all the reports think that Phishing / social engineering attacks and Malware / Ransomware attacks rank very high on those lists [18], [26] [27]. Other cybersecurity-related risks/ threats that the financial services sector needs to grapple with

include, Denial of Service attacks (DOSA), Spoofing, data breaches / unencrypted data, supply-chain attacks, cloud security threats, web/ application/ mobile threats [6], [34].

Although most of the operations, products and services in the financial sector are based on risk (operational risk) and assessment and decision-making, the challenges of technology and digitisation add a different category of risks that must be understood and adequately mitigated for the banks to remain operational and resilient. Some of the countermeasures that have been implemented to mitigate these risks and threats are generally categorised into any of the following technological, technical, organisational, administrative, physical, people and legal/regulatory [6], [14], [35] they include tightening internal security, conducting assessments and audits, providing cybersecurity training and awareness programs [28], proactive monitoring, creating a cybersecurity culture, and cross-sector collaboration [29] as cyber threats evolve, continuous updating of cybersecurity frameworks, policies and strategies are crucial [29], for example, the just updated PCI-DSS and ISO27001 frameworks to cater for changes including cloud computing and emerging technologies.

2.1.3. Cybersecurity Measures in Banking

Fundamental to effective cybersecurity is Risk Management. Information / Cybersecurity itself primarily entails ensuring the Confidentiality, Integrity, and Availability (C.I.A) of Information assets. Information /Cybersecurity risk management is the process of managing risks (threats and vulnerabilities) associated with information technology. It involves identifying, assessing, and treating the risks to the confidentiality, Integrity and availability of an organisations asset. Risk management which consists of risk assessment and risk treatment provides the organisation with a framework, for example NIST CSF 2.0 which is made of six (6) core functions (Govern, Identify, Protect, Detect, Respond, and Recover) provides a risk-based framework [15] for making informed decisions to enable it to strike the right balance that can be achieved between competing variables (threats, opportunities, cost and benefits) to deliver the best business objectives [36]. Risk management is fundamental to successfully defending an organisation's assets, it helps the organisation to protect what is important to them. Many studies identified risk management as a crucial measure for cybersecurity within the banking and financial sector emphasising the need to have a risk management strategy, cybersecurity incident response plans, and mechanisms to mitigate future cybersecurity events [37] some other studies have expanded the scope of risk management to include third-party risk arguing that the provisions of the banks which are now more interconnected and dependent or other providers than ever [38] some other studies emphasised the need for cyber intelligence in risk management, recommending that financial institutions monitor organized crime and dark web

threats [39], emphasis has also been made on the need for mandatory incident report arguing that there are currently insufficient risk data suggesting underreporting of cybersecurity incidents [40].

Information sharing and threat intelligence are different concepts that are both aimed at the collective defence effort against cyber threats. A UK government-published guidance on cyber-threat intelligence states that information sharing will "significantly assist organisations mutually to pre-empt, prevent, detect, and respond to serious cyber incidents and threats while improving the preparedness and resilience of the wider ecosystem". This emphasises the critical role information sharing plays in defending cyberspace and has been identified as part of pillar 5 (countering threats) of the UK National Cybersecurity strategy policy paper [41]. Many of scholars have identified the need for information sharing to be embedded into the risk management framework given the increasing reliance on third-party systems/ suppliers to offer digital services [39], [40], [42]. As straightforward as the requirement may seem initially, one study while conducting a cyber defence exercise on these challenges using a case study of two live international cybersecurity exercises in 2018 and 2019 identified that lack of knowledge on sharing standards and experience of the professional are some of the factors that hampers information sharing [43]. This is suggestive that the more experienced the professional is, the more comfortable or confident they may be at information sharing. It is not very clear whether this observed and analysed behaviour and attitudes of participants representative of all cybersecurity professionals.

Incident response is part of the "Respond" capability in the NIST CSF, this function if implemented correctly gives the organisation the ability to respond to a series of incidents that they would have pre-empted and practised different response strategies for. The capabilities of the Respond function in NIST CSF are response planning, Communications, Analysis, Mitigation and Improvements. As part of the communication capability the organisation experiencing a cyber incident would have had a list of organisations and their reporting requirements for any incident the organisation maybe facing, e.g. an organisation that has suffered a data breach from a cyberattack must report to the ICO within 72 hours of knowing of the attack [44]. To be able to achieve these reporting requirements or similar, the organisation needs to have structures and systems in place that will be followed when and if the situation arises, this is why good and effective cybersecurity is built on the three (3) pillars of people, process, and technology. The laid down processes to be followed and the technology that may have been deployed to detect and alert on information security event (occurrence indicating a possible breach of information security policy or failure of controls, or a previously unknown

situation that may be security relevant) or incident (single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security) will need to be managed by people who are trained to use these resources effectively. In short security training and awareness programs play a key role in establishing and maintaining an effective cybersecurity program.

It can therefore be concluded from above measures that effective cybersecurity in banking depends on robust risk management focusing on the confidentiality, integrity, and availability (CIA) of information assets. This involves developing risk management strategies, incident response plans, techniques and mechanisms to mitigate cyber threats, with an emphasis on third-party risks and the integration of cyber intelligence and information sharing and information sharing and threat intelligence are critical for pre-empting and responding to cyber incidents, but challenges remain in standardizing and encouraging these practices across professionals.

2.2. Cybersecurity Frameworks and It's effectiveness in the Banking Sector

2.2.1. Major Cybersecurity Frameworks in the Banking Sector

The banking sector has experienced the development of various regulatory frameworks and standards aimed at mitigating cyber threats, notably the Basel III standards, the PCI-DSS, and the ISO/IEC 27001. Research has demonstrated that these frameworks significantly reduce the incidence of cyber breaches when rigorously adhered to. Sulistyowati et al. [45] contend that the "measure of an adequate level of protection is an indicator of the cybersecurity awareness aspects of an organisation's business processes."

Risk management, an integral part of combating cyber threats, comprises risk assessment and mitigation. Dawodu et al., [46] and colleagues elaborated on cybersecurity risk assessment as a process encompassing identifying, analysing, and evaluating threats and vulnerabilities that could impact the confidentiality, integrity, and availability of banking systems and data. They stress the necessity of a robust cybersecurity regime that meets internal and external requirements by aligning risk assessment methods with industry-specific regulations and compliance standards. In a related study, Adegbite et al., [47] and colleagues consider the dynamic nature of cyber threats and their potential impact on critical financial infrastructure, stressing the essential nature of ongoing risk identification, assessment, and mitigation strategies to adapt to these evolving threats and vulnerabilities. Both studies, albeit from disparate angles, concur on a multifaceted risk management approach that extends beyond individual entities and aligns with regulatory and compliance frameworks. A risk-based cybersecurity strategy is pivotal for tailoring controls to an organization's unique situation. The

consensus in the literature reviewed affirms that risk management is foundational in understanding and shielding against cyber threats. Numerous risk management frameworks have been devised to aid organizations in this endeavour, focusing on various types of risks and purposes.

There are two (2) possible extremes in the design of cybersecurity frameworks, they are principles-based design and prescriptive-based design. A framework will usually follow either of these designs or it will be a mixed approach, having elements of both design approaches. The design method usually has a significance on the choice of compliance and the consequences of non-compliance. Principles-based design is one where the focus is on the intention or the goal that is to be achieved. It states the intention and leaves it to implementers to interpret and attempt to achieve the law however they can. They use general languages and statements that are technology-averse to state the goal or intention of the law or regulation without necessarily stating the how and what, to achieve it. It also uses subjective, or qualitative language such as fair, logical, reasonable, suitable, etc. Contrastingly, a prescriptive-based law uses specific terms and is often not technology-neutral. They tend to be more specific, for example, PCI DSS requirement 8.3.6 states: "If passwords or passphrases are used as authentication factors it must contain a minimum length of 12 characters and both numeric and alphabetic characters" [16].

This analysis will concentrate on NIST CSF, ISO27001/2, and PCI-DSS and the other frameworks in Table 1 below, comparing the frameworks based on origin, applicability/scope, focus, incident response reporting, privacy requirements, breach notification, continuous improvement etc. The advantages of these frameworks include identifying and mitigating risks, aiding organisations in complying with relevant regulations and laws, and facilitating collaboration and communication among stakeholders. Conversely, challenges include the complexity of implementation and maintenance, the risk of degenerating into a checkbox exercise for compliance certification, and the critical need for senior leadership buy-in for effective implementation [47]. The NIST CSF offers a structured framework for implementing adequate security controls, highlighting its standardised approach to cybersecurity. A more in-depth comparison of the frameworks is contained in the table below (table 1). Although it is possible to map the frameworks to each other to remove duplication of efforts especially if there is a need to comply with more than one framework. In a nutshell, the banking sector depends majorly on various regulatory frameworks, particularly PCI-DSS, ISO/IEC 27001, and NIST CSF to mitigate cyber threats. These frameworks have proven effective in reducing

and mitigating cyber and data breaches when rigorously followed, with risk management being a critical component for aligning security measures with industry-specific regulations.

Table 1: Frameworks Comparison table

Criteria	NIST CSF v2.0	ISO/IEC 27001/2	PCI DSS v4.0	CIS Controls v8.1	GDPR 2018	UK DPA 2018	PRA Cyber Resilience
Origin	U.S. (NIST)	International (ISO/IEC)	International (PCI Security Standards Council)	U.S. (CIS)	European Union	United Kingdom	United Kingdom
Description	It is It includes a set of common activities and desired outcomes to improve security and resilience across critical infrastructure sectors.	is a ISO 27001/27002 are family of frameworks developed by the International Standards Organization (ISO) for information security, cybersecurity and privacy protection helps organizations keep information assets secure.	Owned and created by PCI DSS is owned and created by the Payment Card Brands (Mastercard, Visa, American Express, JCB, Discover, and China UnionPay).	Cybersecurity best practices	GDPR regulation is an EU law on data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.	Governed by the Information Commissioner Office (ICO). The UK DPA 2018 implements those parts of the GDPR which 'are to be determined by Member State law' and it creates a framework similar to the GDPR for the processing of personal data which is outside the scope of the GDPR.	Prudential Regulatory Authority (PRA – part of Bank of England). Prudential Regulatory Authority (PRA) Cyber Resilience is a set of Cyber Security questions, PRA regulated entities are expected to focus on.
Purpose	Improve cybersecurity risk management. It enables organisations to apply a risk-based approach to managing information security.	Information Security Management System (ISMS) and Certification program	Protect payment card data. It is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing — including: Merchants, Processors, Acquirers, Issuers and Other service providers.	CIS CSC consists of a set of best practice information security controls presented as a prioritised set of actions which enable organisations to defend against common information security threats.	Protect personal data and privacy	Aligns with GDPR to protect personal data. The UK implementation of GDPR	Assess and enhance cyber resilience in financial institutions
Focus	Cybersecurity	Information Security	Payment Card Data Security	Cybersecurity hygiene	Data Protection and Privacy	Data Protection and Privacy	Cyber Resilience in Financial Institutions
Structure	6 Core Functions, 22 Categories, 106 Subcategories	4 Categories, 93 Controls (ISO 27001:2022)	6 goals, 12 requirements, and over 300 controls.	18 Controls, 153 Sub-controls	11 Chapters, 99 Articles, Over 173 Recitals	7 Principles, 99 Articles	395 Questions (approx.) covering various areas
Applicability	Voluntary, primarily U.S. critical infrastructure but globally adopted	Global, all industries	Global, all entities handling card payments. Whether any entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (such as payment brands and acquirers).	Global, all industries	Mandatory for organizations processing EU residents' data	Mandatory for UK organizations processing personal data	Mandatory for UK-regulated financial institutions
Certification	No formal certification	Certification available (ISO 27001)	Certification available (PCI DSS)	No formal certification	No certification, but compliance is required	No certification, but compliance is required	No certification, but compliance is required
Risk Management Approach	Risk-based, adaptive	Risk-based, prescriptive	Risk-based, prescriptive	Risk-based, prescriptive	Risk-based, with a focus on data protection impact assessments (DPIAs)	Risk-based, aligned with GDPR	Risk-based, with a focus on resilience and response
Flexibility	Highly flexible, adaptable	Structured, with some flexibility in implementation	Structured, with specific requirements	Flexible, adaptable to organizational needs	Less flexible, specific legal obligations	Less flexible, specific legal obligations	Flexible, tailored to the institution's size and complexity
Global Recognition	High, especially in the U.S. and sectors like critical infrastructure	High, especially in regulated industries	High, especially in payment processing	High, used globally	High, especially in EU and globally for data processing	High, especially in the UK	Recognized within the UK financial sector
Primary Audience	Organizations of all sizes	Organizations of all sizes	Organizations handling card payments	Organisations of all sizes	Any organization processing EU residents' data	Any organization processing UK residents' data	Financial institutions regulated by the PRA
Data Protection Focus	Indirect	Indirect	Direct, focused on payment card data	Indirect	Direct, focused on personal data	Direct, focused on personal data	Indirect, focused on operational resilience
Incident Response Requirements	Yes, as part of the "Respond" function	Yes, part of ISMS (ISO 27001)	Yes, in several requirements	Yes, as part of the controls	Yes, with mandatory breach notification	Yes, with mandatory breach notification	Yes, emphasis on preparedness and response
Privacy Requirements	Not a primary focus	Not a primary focus	Not a primary focus	Not a primary focus	Core focus	Core focus	Privacy is part of broader operational resilience
Data Breach Notification	Encouraged, but not mandatory	Not explicitly covered	Yes, as part of incident response	Strong emphasis on continuous improvement	Mandatory within 72 hours	Mandatory within 72 hours	Yes, part of incident response and regulatory reporting
Focus on Continuous Improvement	Strong emphasis, adaptive and evolving	Strong emphasis, PDCA cycle	Continuous monitoring and improvement	Continuous compliance	Continuous compliance	Continuous compliance	Strong emphasis on testing and improving resilience

2.2.2. Effectiveness of Cybersecurity Frameworks in the Banking Sector

The financial services sector is heavily regulated; there are a variety of regulations and policies that must be adhered to across the different sections of the sector, for example there are frameworks that the banks must comply with for processing customer data, the Data Protection Act (DPA) and GDPR and it numerous variations across the world, the Money Laundering and Terrorist Financing Regulation [48] in UK Financial Conducts Authority's CBEST [49] or the Bank of England's CQUEST [50]. Many cybersecurity frameworks are usually implemented within the sector to protect the internet and communications systems and technologies that

enhance several activities. The effectiveness of these cybersecurity frameworks within the banking sector has been the subject of many debates; some scholars think that these frameworks are indispensable when it comes to the matter of safeguarding the data, assets, systems and infrastructures within the sector and achieving cyber resilience, on the other hand, some scholars believe that the regulatory and compliance expectations from these frameworks often are too numerous and sometimes duplicates of each other and most importantly they may impede innovation and competition. An example of a mandatory framework for any operators in payment services within the financial sector is the PCI-DSS; it imposes specific requirements for shielding credit card data and has been embraced by financial institutions on a global scale. It is very important to understand the effectiveness and the benefits of these cybersecurity frameworks, especially as reliance on digital technologies and the corresponding rise in cyber threats and cyberattacks is almost a daily occurrence, the importance of this research cannot be overstated. Researching the banking sector of Kazakhstan, Buzaubayewa et al. [32] emphasised the significance of regulatory compliance in enhancing the risk management capabilities of banks. they conclude that regulatory compliance has a direct relationship with financial performance. Their findings indicate a direct correlation between regulatory compliance and risk management, suggesting that compliance efforts significantly strengthen risk management capabilities. Moreover, adherence to cybersecurity regulations is emphasized as a means to improve the protection of financial digital assets against cyber-attacks [51]. Interestingly, while regulatory frameworks are crucial for maintaining financial stability and consumer protection, they also need to balance the promotion of innovation within the banking sector. The comparative review of digital banking regulations between Nigeria and the USA highlights the differences in regulatory focus, with Nigeria emphasizing financial inclusion and the USA prioritizing consumer protection and competitive markets [52]. Additionally, the convergence of global cybersecurity standards suggests a trend towards harmonized regulatory approaches, despite regional differences in data protection and breach notification [53]. In summary, the literature underscores the importance of robust regulatory frameworks and security standards in the banking sector. Effective regulatory compliance not only strengthens risk management and financial performance but also protects against cyber threats. However, the challenge lies in crafting regulations that safeguard the financial system and consumers while fostering innovation and adapting to technological advancements. To achieve this, a balanced and dynamic approach to cybersecurity, incorporating advanced technologies and continuous risk assessment, is recommended [54] [53].

2.2.3. Criteria for Effectiveness

There are a variety of ways by which the effectiveness of adopted cybersecurity frameworks can be measured within an organisation. One of the easier ways of assessing effectiveness is if the organisation has subscribed to the compliance programme e.g., the ISO/IEC 27001, which is a certification program; the requirement for certification may be that the regulation audit is completed by a certified assessor who is external to the organisation, can assess the organisation and report on the effectiveness of their controls /cybersecurity programme. Although it is possible to adopt the framework but opt out of the certification program, in which case the organisation will be adopting ISO/IEC 27002. Some other organisations that operate in specific sectors, and operate at a specific level, are mandated to have a regular external assessor to audit their applicable cybersecurity program annually; an example is the PCI-DSS requirement for organisations that process over 6 million transactions annually to engage a qualified security assessor (QSA) to assess their level of compliance to the PCI standard [55]. In some other instances, if an organisation has suffered a breach or for some other reasons on their acquirer's demand, they may have to be subject to a high level of assessment by a QSA to assess their cybersecurity posture and compliance.

Another way organisations that have the resources assess their own cybersecurity effectiveness is by completing an internally conducted self-assessment implemented controls using a maturity model. A popular adopted maturity model in cybersecurity is the Capability Maturity Model Integration (CMMI) which is a risk management process that helps organizations to assess the maturity of the process and offers guidance on how it can improve. There are five (5) maturity levels or capability levels in the model; level is Initial (processes are unpredictable and reactive), level 2 is Managed (repeatable), level 3 is Defined (processes are proactive, rather than reactive), level 4 is Quantitatively managed (processes are measured and controlled), level 5 is Optimized (processes are stable and flexible) [56].

Incident management and reporting is another parameter that organisations use to monitor their effectiveness; having a robust incident management program which is a subset of an overall cybersecurity program, reduces the impact of cyber incidents [57].

2.3. Cybersecurity in Decentralized Finance (DeFi).

2.3.1. Overview of Decentralized Finance (DeFi)

Decentralized Finance (DeFi), concept describes a concept that utilizes Distributed Ledger Technology (DLT) in providing financial services in a way that trading, lending, and investing are done without the need for a traditional central intermediary [45]. DeFi merged with the promise of providing financial services through a combination of infrastructure,

markets, technology, methods, and applications without intermediaries, a contrast to what is on offer through traditional financial institutions. Technology is used to facilitate and enhance interactions between multiple participants, intermediaries, and end-users, who are spread across multiple jurisdictions. Although the term "decentralized" is generally considered to be ambiguous, there is a broad agreement that it refers to services that are provided by multiple parties, including participants, intermediaries, and end-users, not the traditional providers as it exists historically i.e., clearing and settlement houses, who are legally dispersed across the globe. DeFi describes the technological advancements within the financial sector that utilize decentralisation, blockchain technology, distributed ledger technology, smart contracts, non-intermediary transactions, and open banking; examples are Bitcoin, Stablecoins, etc.

DeFi, though an emerging financial paradigm is built on blockchain technology, offering peer-to-peer financial services without traditional intermediaries ([34]; [58]). DeFi applications utilise smart contracts to enable various financial activities, including lending, borrowing, trading, and insurance ([59]). The fundamental principles of DeFi include decentralisation, disintermediation, and user empowerment [39]; [60]. While DeFi presents innovative opportunities, it also faces challenges such as security risks, market manipulation, and regulatory concerns ([58]; [61]). To address these issues, researchers propose principles for DeFi disclosure and regulation, emphasising the need for a common disclosure platform and appropriate governance mechanisms [62]. As DeFi continues to evolve, it has the potential to transform the financial landscape, but stakeholders must carefully consider the associated risks and implications for financial stability ([63]; [59]).

The DeFi ecosystem, a viable alternative to traditional banking, comprises several key components and technologies. These include smart contracts, decentralized exchanges, stablecoins, lending and borrowing platforms, decentralized finance applications, blockchain-based identity verification, and decentralized autonomous organizations (DAOs). Each of these components and technologies plays a crucial role in enabling the DeFi ecosystem to function effectively. Together, they form the foundation of this innovative financial system, which has gained significant traction in recent years. The DeFi ecosystem has emerged as a legitimate and increasingly popular alternative to traditional banking and financial systems. As the technology continues to advance, the DeFi ecosystem will likely become even more integrated and accessible to users across the globe, potentially revolutionising the way we think about and interact with financial transactions. The acceptance of DeFi as an alternative to conventional banking is not without its challenges; different governmental bodies across the world do not have an equal level of acceptance of it; while some have embraced it and are making provisions

for it in their policies, others have outrightly banned it, declared it illegal or completely ignored it, yet some other have taken the approach of caution and scepticism [64].

The key components and technologies of the DeFi ecosystem, as an alternative to traditional banking, include blockchain technology, smart contracts, decentralised applications (dApps), and various financial protocols. The blockchain serves as the foundational layer, providing a decentralised and transparent ledger for all transactions. [65]. Smart contracts automate and enforce the terms of an agreement without intermediaries, which is crucial for the functioning of DeFi platforms. [66]. Decentralized applications (dApps) run on top of the blockchain, enabling a wide range of financial services such as lending, borrowing, and trading through user-friendly interfaces [67]. Interestingly, while DeFi aims to replicate and improve upon traditional financial services, it also introduces unique features like tokenization (usually categorized as fungible, non-fungible, and semi-fungible), which allows for the creation of digital assets that can represent real-world assets or rights [68]. Decentralized exchanges (DEXs) facilitate the trading of these assets without the need for a central authority [69]. In summary, the DeFi ecosystem is built upon integrating blockchain technology, smart contracts, dApps, and financial protocols that collectively offer a decentralized alternative to traditional banking. These components work in concert to provide a transparent, open, and interoperable financial infrastructure [67] [65]. While DeFi presents opportunities for innovation and inclusivity in financial services, it also faces challenges related to security, governance, and regulatory compliance that must be addressed as the ecosystem evolves [69].

2.3.2. Cybersecurity in Decentralized Finance (DeFi)

Decentralized Finance (DeFi), devoid of centralized oversight and based on blockchain technology, introduces distinct cybersecurity challenges that diverge from traditional finance systems [70] and delineates the unique cyber threat landscape in DeFi, underscoring the imperative for customized security measures. The extension of conventional banking security protocols to DeFi platforms is a nascent field, with initial investigations indicating the necessity for modifications that reflect these systems' decentralized infrastructure.

DeFi, propelled by Decentralized Ledger Technology (DLT), is an emergent and rapidly progressing domain within the banking and financial sector, laden with distinct challenges. Despite these challenges, DeFi promises to revolutionize traditional financial services by leveraging decentralized networks to create trustless and transparent protocols that operate without intermediaries [71]. However, Liu et al.,[72] scrutinize mainstream DeFi platforms, revealing concerns regarding the reliability of oracles—entities that are supposed to act as trusted data sources. They pinpoint frequent operational failures and vulnerabilities within the

platforms, advocating for greater transparency, accountability through cryptographic incentives, and enhanced operational robustness. Werner et al., [73] distinguish between technical and economic security within blockchain-based peer-to-peer financial systems, offering a novel functional categorization and definitions of associated risks. Their research delineates areas necessitating a comprehensive understanding of both technical and economic risks.

Kaur et al, [11] characterize DeFi as an avenue for disintermediating financial services using conventional and innovative methods and systematically assessing the attendant risks. They categorize these risks into Operational, Technical, Financial, Legal Regulatory, and nascent risks. Through comparative analysis, they establish technical risks as paramount, followed by legal, regulatory, and financial risks. They argue that stringent regulations might be counterproductive for DeFi's burgeoning sector, instead advocating for a regulatory focus on financial crimes, smart contract vulnerabilities, transactional hazards, and liquidity concerns. Kaur et al, [11] called for a collaborative approach among stakeholders to realize DeFi's full potential without hampering its growth.

A plethora of studies have been dedicated to evaluating the array of cybersecurity standards, regulations, and directives, particularly regarding their efficacy in the banking sector. Srinivas et al., [74] explored these standards as instruments for cyber defence, revealing several challenges to their standardization. These challenges encompass organizational impediments, a lack of responsiveness in standard development, the confusion arising from competing standards, and economic considerations. Their analysis contributes significantly to the discourse on the implementation of cybersecurity measures within the financial sector.

Existing scholarship has laid a considerable foundation for the understanding of cybersecurity within the banking sector and Decentralized Finance (DeFi), yet there are notable gaps. Some researchers posit that in the realm of traditional banking, global regulations are lagging. Didenko [75] observed that bespoke cybersecurity laws have supplanted general risk management and business continuity rules in several jurisdictions, including the European Union, Hong Kong, Russia, the USA, and Singapore. Despite advancements, Didenko [75] contends that cybersecurity regulation requires further development, facing challenges such as the delineation of cybersecurity risk from operational risks, establishing minimum standards for cyber-event reporting, formulating a comprehensive cross-sectoral cybersecurity strategy, managing third-party risks, ensuring rapid updating of current knowledge, determining accountability for regulators, and instituting adequate penalties and enforcement mechanisms.

Piehani [76] critiques the Basel framework's operational risk model as inadequate for addressing the intricacies of cyber risk. This critique underpins a broader concern regarding the absence of cohesive international cybersecurity laws and the complexity of legal interpretations within individual nations. This situation in traditional banking raises questions about the potential replication of these issues in the regulation of the DeFi ecosystem.

2.3.3 Cybersecurity Threats and Unique Challenges in DeFi

A complete implementation of DeFi has five(5) distinguishing characteristics: Self-control, Permissionless, Programmability, Transparency and Composability [77]

The Permissionless characteristic of DeFi is its openness to everyone, anyone with a crypto wallet and an internet connection can access DeFi applications from any location. This feature has been identified as a major contributor to the cybersecurity challenges in the ecosystem as a whole. It has been suggested that small and Medium businesses, which often as adopters, engage with DeFi as an alternative to challenges of traditional banks, often do so without adequate understanding of the underlying technology coupled with poor security hygiene practices on their part and a general lack of investment and skill makes them easy and profitable targets to cyberattacks exploiting their vulnerabilities [78]. Other cybersecurity challenges confronting the DeFi model are smart contract vulnerabilities, liquidity pool attacks, and oracle manipulation [79], some risks have also been identified and researched by many academics. Although not all of them are relevant from a cybersecurity perspective, the risks have been broadly categorised as financial risks, technical risks, operational risks [79], regulatory risks, Liquidity risk, market risk and smart contract risks [80].

However, criminals have exploited this feature to conduct many cyber-enabled nefarious activities and cyber currency crimes, including money laundering. A major cybersecurity challenge for the DeFi model is the lack of central governance/regulation, a key element of decentralization. DeFi was initially presented as a way to promote the democratization of finance [65]. Unfortunately, this feature has been exploited by criminals for various malicious cyber activities, including money laundering. The value of laundered cryptocurrency in 2021 was valued at $8.6B, a 30% increase from the 2020 value of $6.6B [81]. There have been many crypto cyber-attacks with deadly impact, but the five (5) largest attacks are; the $610 Million heist that exploited the vulnerabilities in the Poly Networks systems in 2021, the gamer heist attack on Ronin Network, a platform that allows gamers to collect and trade in non-fungible tokens (NFTs) resulting in a loss of $540 million in Ethereum and USD Coin tokens in 2022, $532 million, Coincheck attack in January 2018, $480 million Mt Gox, in February 2014, and $334 million Wormhole in February 2022 [82], [83].

2.4. Applicability of Banking sector Cybersecurity measures to DeFi Platforms

2.4.1. Critical Analysis – Current State of Knowledge

The operational paradigm of banks and financial institutions has undergone a dynamic evolution, with an increasing transition to virtual service delivery via interconnected networks and digitization, this has massively increased the attack surface, making these institutions more susceptible to a variety of information technology threats, including malware, social engineering, and broader cyberattacks [84]. Given the critical nature of financial infrastructure to societal well-being, the sector is heavily regulated and recently upgraded to Critical National Infrastructure status [6].The frequency and sophistication of these cyber threats reflect the motives of various actors. An IMF blog post in April 2024 reported that of the over 20,00 cyberattacks in the financial sector, almost 10,000 of them were targeted against banks [85]. including state-sponsored entities, as evidenced by incidents such as the DDoS attack attributed to Moscow against Ukrainian banking and government infrastructure in February 2022 [86].

In light of these risks, there has been significant scholarly and empirical research aimed at understanding, categorizing, and countering the threats faced by the banking and financial sectors. The inception of cybersecurity within these sectors was a strategic response to the necessity of protecting this infrastructure, initially adopting a defensive posture focused on safeguarding against external threats. Over time, this has evolved into a regulatory framework, now an industry standard, acknowledged by scholars as essential for the effective protection of technological assets [74].

The proposed cybersecurity framework by Darem et al. (2023) [6] is intended to guide the development of efficient defensive strategies within the banking sector, promoting a shift from a reactive to a proactive stance in cybersecurity and resilience. This proposition is supported by AlBenJasim et al. [87] who, through a case study of financial institutions in Bahrain, identified common elements across international frameworks and standards, suggesting that the creation of a cybersecurity framework could provide a valuable new perspective and an extension of existing knowledge.

The literature consistently underscores the importance of risk management as a defence strategy, with Darem et al.[6] emphasising the need for a layered cybersecurity approach integrating technical, legal, and organisational measures. [88] Advocates for a 'holistic risk management' approach, incorporating strict internal processes, external professional support, and insurance strategies. Additionally, frameworks for understanding and developing new and evolving risks, especially those associated with virtual and cryptocurrencies, have been proposed from a regulatory standpoint. [89].

Both CeFi and DeFi given the criticality of the services they provide face similar types of risks including operational risks, market risks including price manipulation, liquidity risks, governance and regulatory risk [10],[90],[91]. Both traditional banks and DeFi offer financial services such as interest-bearing accounts, loans, assets, and trading facilities. A major difference between both types of institutions is in the way those services are offered, in traditional banking which is sometimes referred to as CeFi (Centralized Finance), their offering is centralized, controlled by specific heavily regulated players performing specific functions e.g., clearing houses, the banks themselves. DeFi on the other hand promises to provide financial services without intermediaries by eliminating centralization, this allows many participants (intermediaries) to be involved in the transactions with the advantage of transactions being completed in near real-time as possible compared to CeFi. Although DeFi promises decentralization, some scholars have questioned whether DeFi offers true decentralization given its practical implementation. In her article, Walch [10] purports that the issue of decentralization is a matter of power concentration, saying that it is possible on Blockchain systems to have sites of concentrated power which is similar to traditional financial institutions [10], this has been referred to as the "Decentralisation illusion" [90]. Alonso et al.,[90] while supporting the concentration of power argument identified inevitable centralization as another reason for their claim that decentralisation is an illusion, stating that this is the case since all DeFi platforms have their central governance frameworks for making strategic and operational decisions. To support this argument, in their work on a study of web measurements of the security, privacy, and decentralization properties of popular DeFi front ends, Winter et al., [92] found that many DeFi sites rely heavily on centralized infrastructure, with providers like Cloudflare hosting 44% and AWS hosting 38% of the 78 sites they analysed. Centralization in DeFi may initially appear to be a bad thing or a failure of DeFi, for example, consider the impact of a successful DDoS attack on Cloudflare and AWS or a phishing attack on the users of those sites, but when this is considered from the perspective of exploiting those similarities (the clusters /centralization) to proffer the much need cybersecurity controls it may go a long way in the challenge of regulatory oversight which has been identified to be either lacking or insufficient.

Cybersecurity frameworks provide a system of consistent and repeatable guidelines, standards and best practices to organisations of different sizes, sectors and maturity to manage their information security, cybersecurity and privacy risks [14], [15]. Though focusing on risk management and regulatory compliance aspects of the frameworks, adapting banking cybersecurity frameworks to the DeFi space poses difficulties as it requires a risk management

strategy in DeFi and tackling emerging compliance risks related to financial crimes. The cybersecurity frameworks that are popularly adopted in the banking sector are mostly general frameworks, they are not specific to the financial sector (e.g., ISO27001 and NIST CSF) their applicability has been scholarly researched.

For this research, the similarities and differences between CeFi and DeFi in regards to cybersecurity are considered in the area of the risk management of the threats to the financial stability and resilience of both types of service delivery of products and how this can be mitigated. It has been established that similarities exist not only in the products and services but also in the implementation of both types of service delivery. i.e., a degree of centralization existing in both CeFi and DeFi, it may immediately seem from this perspective that it is possible to apply a similar CeFi cybersecurity framework to DeFi, but after careful review of the scholarly work in this area, it is evident that there is a divergence of opinion. While some studies suggest the possibility of adopting this framework [93], [94], they have further suggested that existing standards require significant revisions before they can be fit for purpose proposing a new set of standards that addresses both CeFi and DeFi [94]. Having identified potential defences (time-based defences, code analysis, and monitoring of centralized exchange interactions), Zhou et al., concluded that there is a plausibility that existing security standards could be adapted to address the security needs of the DeFi environment [12]. Other works on the matter of adaptability discussed the matter from the perspective of regulatory oversight [93]. It has been suggested that “regulatory oversight should focus on developers and validators who control the network protocol” [93] suggesting that once compliance is established at this level, many other functions can be built to address the majority of other issues. A yet different perspective was presented by Wronka, while acknowledging the importance of GDPR and the need to comply with data protection laws across the globe, was not convinced that simply applying existing standards was enough, but suggested that new technological solutions may be needed to address compliance and security issues in DeFi [95]. Walch cautioned about the need for a deeper understanding of how power operates in each specific blockchain system rather than applying blanket assumptions based on the term "decentralized" before making legal or regulatory decisions. She advocated for an approach that is more nuanced and fact-based, such that will take into consideration the roles and actions of key actors e.g. core developers and significant miners within the system who possess and may wield concentrated power in the regulation-making process [10]. Adopting existing banking sector cybersecurity frameworks to the DeFi environment is challenging due to the generalized nature of current frameworks, the unique risks and compliance issues in DeFi, and the need for a different

approach to risk management. These challenges highlight the necessity for developing tailored cybersecurity strategies that address the specific needs and threats of the DeFi ecosystem.

2.5. Gaps and Future Research Directions

2.5.1. Summary of Key Findings

As the above shows, a dynamic interplay exists between technological advancements and cybersecurity challenges within the banking sector. The pivotal role of stringent regulatory frameworks, such as NIS2 and DORA (which currently are at the infancy stage compared to Standards such as NIST CSF and PCI-DSS, which have seen many iterations of updates and reviews) and various cybersecurity standards, in fortifying the sector against escalating cyber threats cannot be overemphasized. The literature review accentuates the banking sector's recognition as Critical National Infrastructure (CNI), highlighting the profound societal repercussions of potential cybersecurity breaches.

One of this study's main contributions to knowledge is its examination of the adequacy of existing security protocols and the fit of DeFi in developing tailored security measures reflective of decentralized architecture. This discussion is instrumental in broadening the academic discourse, offering insights into the intersection of cybersecurity and blockchain technology within financial systems.

Another key contribution is the examination of various cybersecurity frameworks and standards, such as the NIST Cybersecurity Framework, ISO/IEC 27001, and PCI-DSS, elucidating their significance in the banking sector's risk management strategies. The study's comparative analysis between these frameworks and their applicability to both traditional banking and DeFi illuminates the nuanced complexities and requisite adaptability of cybersecurity measures in the evolving financial landscape.

Furthermore, the review identifies critical research gaps, particularly the need for comparative analyses between traditional banking and DeFi's cybersecurity frameworks and a deeper exploration of the rapid evolution of cyber threats. The review catalyses ongoing scholarly inquiry by proposing future research directions, aiming to enhance the understanding and efficacy of cybersecurity measures within the financial sector.

In conclusion, this literature review contributes significantly to the knowledge of cybersecurity in the banking and financial sectors. It offers a comprehensive analysis of the current state of knowledge, highlights the sector's critical vulnerabilities, and proposes future research trajectories to address emerging challenges. The review is a pivotal reference for academics, industry practitioners, and policymakers, aiding in formulating robust cybersecurity strategies to safeguard the financial sector's integrity in an increasingly digitalized world.

2.5.2. Identified Gaps in Literature

This research has revealed a gap in the literature that covers cybersecurity frameworks that are specifically tailored to the DeFi environment. Some existing research covers the challenges of security in DeFi with some proffering ideas of how this risks can be covered. For instance, the IMF recognising the current policy gap recommended the need for a national cybersecurity strategy especially in emerging markets and developing economies recommended that national authorities develop cybersecurity policy frameworks to strengthen the resilience of the financial sector [85].

While more of the available literature on DeFi security is focused on addressing the technical aspects such as vulnerability in smart contracts, and weaknesses in protocols, platforms, and applications, there is even less literature on the cybersecurity frameworks in DeFi. The few that could be considered, are more focused on the compliance aspect of frameworks with very little on cybersecurity risk management as a whole. Some studies were focused on the financial sector as a whole, while examining cybersecurity challenges and solutions in the broader financial sector, including traditional financial institutions and emerging technologies DeFi, Okoye et al., [96] emphasizes the need for comprehensive cybersecurity strategies, regulatory compliance, and technological advancements to address evolving cyber threats in the financial industry as a whole, they identified that there is a need for more comprehensive studies on the integration of advanced digital technologies and their impact on cybersecurity vulnerabilities in financial institutions, advocating for a need for further research to develop a concept they referred to as “anticipatory risk analytics models” that can effectively deal with the complexity and unpredictability of modern cyber threats [96]., Although their focus was on data security, they identified a need for a proactive, dynamic regulatory framework that could cope with the complex and dynamic nature of threats in emerging technologies hinting at collaboration between regulatory bodies and financial institutions. This can be summarised as an opinion that current frameworks are inadequate or ineffective in the face of dynamic and rapidly changing threats. Using NIST to illustrate her point, Goodwin [37], concluded that the voluntary nature and lack of legal mandates of the framework are capable of creating implementation inconsistencies across the sector ultimately limiting its effectiveness.

In summary, the existing cybersecurity frameworks in the banking and financial sector are cybersecurity frameworks that provide basic foundational practices that can be applied to any organisation of any size or sector (NIST definition). These frameworks (both ISO2700 and NIST CSF) are general frameworks that are not specific to the sector, this is a major point in

the challenge of the effectiveness or adequacy of these frameworks, many of the researchers have concluded that hitherto, these frameworks have been instrumental in creating a system of consistent and repeatable security practices, in the present state and going forward, they are inadequacy in the face of rapidly changing threats enhanced by technological advancement.

The other major gap identified is the issue of regulatory compliance. These frameworks mostly do not require mandatory compliance which has been suggested could lead to inconsistencies in implementations making it ineffective across the whole sector, many of scholars are advocating for industry-specific regulatory frameworks. Despite the unanimous support for this idea, there are divergence of opinion on the scope of the implementation with some studies making a distinction between emerging markets in developed and developing countries. Advances in technology which underpins digitization and emerging technologies (e.g. Artificial Intelligence and Machine Learning) have been described as a double-edged sword, many of the studies advocate for the integration of advanced technologies like artificial intelligence and biometrics into cybersecurity measures

2.6. Conclusion

This study into the efficacy of cybersecurity frameworks in the banking sector and their applicability to Decentralized Finance (DeFi) is crucially important in this age of dynamic and evolving digital landscape. As the level of innovation and advancement is constantly changing, and it is often almost impossible to keep up with it; given the sector's criticality, countermeasures to mitigate the new risks and threats must attempt to keep up with the changes. important amid escalating cyber threats. This study endeavours to address the extant scholarly voids, particularly those that pertain to the unique complexities introduced by the decentralized nature of finance. It aspires to enhance the corpus of knowledge about the establishment of rigorous cybersecurity practices that protect the conventional banking milieu and the nascent DeFi domains.

The debate on the necessity and impact of regulatory technologies (RegTech) in the Financial Technology (FinTech) sector is multifaceted. Javaheri et al., [97] acknowledge the foundational role of RegTech in the banking and financial domain; however, they highlight its conspicuous absence in DeFi implementations, such as cryptocurrencies. Conversely, Kaur et al., [11] suggest that stringent regulations could potentially impede the growth and evolution of DeFi. This dichotomy in viewpoints underscores the need for a nuanced approach to regulation in the digital finance landscape, balancing the imperative for security with innovation and expansion.

At a time when cybercrime is escalating, this research to assess how effective cybersecurity frameworks are within banking and whether they can even apply safely also for Decentralized Finance (DeFi) could not be more critical. The purpose of this study is to help fill gaps in the existing literature, particularly concerning issues that are unique due to decentralized finance. This aims to contribute to expanding the knowledge base on creating and enforcing strong security formulas around traditional banking setups, alongside novel DeFi dimensions.

Chapter 3. Research Methodology

3.1. Overview

3.1.1. Methodology approach

In order to research this project topic on the effectiveness of cybersecurity frameworks in the traditional banking sector and its potential applicability to DeFi, the study could be conducted using either the qualitative, quantitative or mixed-methods research design. When studying the effectiveness of cybersecurity frameworks, in the banking sector and their relevance to DeFi researchers can choose between qualitative, quantitative or mixed-methods research designs. Qualitative research is the research type that is focused on exploring and understanding the meaning of certain concepts or phenomena. It is used for finding themes and patterns in a data set to derive a theory, data is gathered through interviews, focus groups, observations etc., with questions such as “Why”, “How”, “In what way” etc. For example, ask participants in an interview “Why do you think cybersecurity frameworks are effective?” Quantitative research involves gathering data through surveys or questionnaires to analyse cause-and-effect relationships between variables. The results are then analysed using logical and mathematical techniques [98]. The mixed-method research methodology combines both qualitative methods to collect and analyse data. Compared to quantitative, qualitative is more of a narrative and is often used to explore or develop a hypothesis, while quantitative is used to test a hypothesis. This approach offers an understanding of the research topic by allowing researchers to examine numerical data alongside in-depth explorations of perspectives, thoughts, attitudes and behaviours. This research could have been completed using any of the three (3) methods described above. Although the mixed method of research would have yielded the most benefit in contributing to knowledge, in my opinion, for this research, it was decided not to go with this method because of time limitations and low participation from respondents. With the mixed method, the researcher can better understand the thought process of the respondents; they can ask further probing questions to gain a better understanding of their perspectives on the applicability of the frameworks and insight into their answer choices.

The mixed method technique would allow for a more comprehensive understanding of the research topic by bringing together the strengths of both methods to achieve a robust and reliable analysis of the data collected. This would have been very beneficial in understanding cybersecurity frameworks' effectiveness on DeFi, which, in comparison to traditional banking, is an emerging and rapidly developing field. DeFi has been described as being in its infancy [99]; its continuous evolution makes it a challenging area to study. As the banking and financial sector becomes more digitized, advancing technologically and innovatively, cybersecurity in

this sector is becoming more developed and defined than in the emerging field of DeFi. The mixed method approach would offer a more complete understanding of the research topic by combining the strengths of both qualitative and quantitative methods to produce a robust and dependable analysis of the collected data.

From the literature review, there is a difference of opinion about the degree of effectiveness of cybersecurity frameworks in mitigating cyberattacks within the banking and financial sector with opinions divided on whether frameworks are adequate and effective or inadequate and requiring further interventions. Some scholars believe that the current popular frameworks (PCI-DSS, ISO27001, NIST CSF) are all effective in providing valuable guidelines and best practices for banks to implement robust cybersecurity measures, but they highlighted the need for continuously updating the framework to match up the constant evolving threat landscape and threat intelligence so the frameworks are dynamic and adaptive [6]. Some other works think these frameworks are not enough by themselves, for instance, though acknowledging the effectiveness of NIST CSF in preventing incidents and strengthening infrastructure, the tool was critiqued because it is only a guideline: guidelines are non-mandatory but voluntary, the author believes this makes it inadequate and advocated for a legal standard from the U.S. Financial Sector so that adoption can be consistent implementation and accountability [37]. Some other scholars argued that the existing frameworks are foundational, questioning the adequacy of the frameworks in fully addressing Fintech-specific concerns and unique risks peculiar to this sector, they however advocated for more Industry tailored frameworks [87].

Given this divergence of opinion, this research set out to gauge to what extent cybersecurity professionals within the sector believe that currently available cybersecurity frameworks are effective in mitigating cyberattacks within the sector. So for this thesis, it was decided to carry out quantitative research, the aim is to gauge the effectiveness of cybersecurity frameworks in the banking sector and their applicability in the DeFi environment. The potential impact of this study's findings on the cybersecurity landscape cannot be overstated. The study examines the efficacy of various cybersecurity frameworks in protecting against cyberattacks in the banking sector and evaluates their potential for application in the decentralized finance (DeFi) ecosystem. The two(2) theories/hypotheses that underlines the development of the data collection questionnaire are the following:

Question 1: Does the implementation of security frameworks significantly reduces the frequency and impact of cyber-attacks in the banking sector?

Question 2: Can Cybersecurity frameworks used in the Banking sector be adapted to effectively mitigate cyber-attacks in DeFi?

Question 3: Do we need new DeFi-specific Cybersecurity Frameworks?

In this section, I discussed the method of collecting, analysing, and interpreting data. The focus of the research which is to examine the effectiveness of cybersecurity frameworks in the Financial and banking sector will proceed by gathering information through a survey on the opinions of professionals using a Likert scale on the effectiveness of cybersecurity frameworks, current state of security hygiene within the DeFi ecosystem, and exploring the feasibility of applying similar Banking Cybersecurity Frameworks to Decentralized Finance (DeFi). While the research has direct implications for the security and stability of the Financial sector as a whole, the study is relevant and important because it will not only provide direction for future research, it could also be seen as a template that can be expanded for such research endeavours.

Conducting quantitative research to examine cybersecurity within the financial sector, which includes both traditional banking systems and the burgeoning field of Decentralized Finance (DeFi), requires selecting appropriate instruments to capture numerical data that can be subjected to statistical analysis. These instruments provide measurable, objective data that complement the nuanced understandings gleaned from qualitative methods. Surveys and questionnaires stand as fundamental instruments in quantitative research. They are designed to collect data from many respondents, allowing for the statistical generalisation of results. For this study, surveys will be crafted to assess the prevalence of cybersecurity practices, the frequency and types of cyber threats encountered, and the effectiveness of various cybersecurity frameworks as perceived by professionals within the sector. Sophisticated statistical tools are then applied to analyse the survey data, revealing patterns, trends, and correlations that might not be visible through qualitative analysis alone.

Another quantitative instrument uses existing databases and records, which hold vast amounts of data related to cyber incidents, including the nature of the breaches, the financial impact, and the recovery time. By applying data mining techniques and statistical analysis to this information, researchers can identify significant patterns and trends over time, contributing to an understanding of the evolving landscape of cyber threats and defences. The first phase of the research will involve a comprehensive literature review to identify the existing gaps in the current knowledge on the topic, followed by a survey of cybersecurity experts to gather their insights on the effectiveness of the frameworks in the banking sector. Additionally, in-depth interviews with key stakeholders in the DeFi space will be conducted to understand their

perspectives on the applicability of these frameworks. The collected data from quantitative methods will be analysed using descriptive statistical analysis techniques and thematic analysis, respectively, with the aim that the findings of this study will provide valuable insights into the effectiveness of cybersecurity frameworks in the banking sector and their potential applicability to DeFi, which can inform the development of more effective and adaptive cybersecurity strategies for these industries.

3.2. Data Collection

3.2.1. Eligibility criteria

To ensure that the sample was representative of the population, I chose to use a non-probabilistic sampling method for this quantitative research. This method allowed me to quickly and efficiently generate a sample that met the study's eligibility criteria which is that participants be cybersecurity professionals. In addition to the ease and speed offered by non-probabilistic sampling, I decided specifically to use the purposive sampling method due to the specific nature of the population being studied and the importance of this criteria in generating a logically representative population.

The data was collected anonymously from two groups of Cybersecurity professionals with varying degrees of expertise working across different sectors and geographically dispersed across the globe. The survey instrument was shared with three (3) WhatsApp groups of cybersecurity professionals. The first group has 91 members, the second group has 166 members, and the third group has 147 members.

The survey was designed to gather the opinions of security professionals with significant work experience in related fields. The survey instrument explored four(4) categorisations to establish participants' expertise in the field of cybersecurity: Less than three years, 3 to 5 years, 5-10 years, and more than ten years. it is assumed that a professional with over three years of experience should be able to have an opinion of whether cybersecurity frameworks are effective or not.

For this purpose, fields considered related to this area of study were traditional banks, specialist financial institutions, digital and online banks, DeFi platforms, Fintech companies, and other regulatory and support institutions. The reasoning behind this selection is that professionals operating within this sector are expected to be closer to the baseline cybersecurity frameworks within this sector, and this will be a criterion for the inclusivity of the data in the analysis.

The survey was designed to gauge participants' expertise based on their experience in cybersecurity. Participants are dispersed across the globe. The survey explored the primary work region of the participants, with options covering North America, Europe, Asia, South

America, Africa and Australia. The purpose of this demographic information is to establish if there is a consensus on which frameworks participants think are essential to their sector across the globe.

This said it must be stated that although organisations operating within this sector are at liberty to choose from a plethora of cybersecurity frameworks, the jurisdiction of both the organisation and its customers plays a significant role in this decision-making process. Jurisdiction also impacts the familiarity and expertise of cybersecurity professionals with various frameworks.

The final eligibility criteria are the current role/responsibility that the participants play within their organisation. The question intends to establish how closely the participants are likely to be working with the frameworks. If the participants are not in any role that could make a decision on the selection of the frameworks or their implementation, their opinion of the effectiveness of the frameworks may not be very accurate and reliable for the purposes of this research.

3.3. Data Analysis

3.3.1. Data Preparation

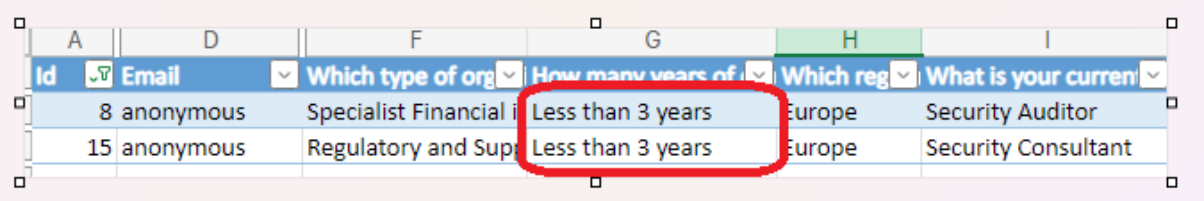
In order to guarantee that the final sample accurately reflected the target population, I made the decision to exclude data from individuals who did not work in financial services or related sectors and to omit any participants who did not possess a minimum of three years of industry experience in financial services. The total number of anonymous data collected was thirty-four (34). Of these, seven 7 (Table 2) responses were excluded from the final data set to be analysed. Five of the participants were excluded because they did not meet the criteria of working in the financial sector (figure 2 below), the other two were excluded due to their level of experience in cybersecurity. The participants excluded from their primary place of work chose the "other" option for the first demographic question about the type of organization they work for. They identified their organisations as higher education, retail, energy, and technology sectors, with one participant indicating "non". The other 2 disqualified responses both indicated less than 3 years of experience (figure 1 below). The decision to excluded the seven responses as explained above will enhance the effort to create a more homogeneous sample that better reflects the target population, which is primarily composed of individuals working in financial services or related fields and having at least three years of experience.

The last exclusion criterion was in Column O, where some participants answered “no” to the question about their familiarity with the DeFi ecosystem (figure 3 below). The decision was made to use this exclusion on the assumption that if the participant is not familiar with DeFi, their responses to questions on the topic are not likely to be reliable. One of the participants

who indicated to be working in a DeFi platform in response to the question of where they worked chose no to the question on their familiarity with DeFi platforms. This instance could have been an error or misunderstanding of either of the questions, but the answers to both questions are contradictory.

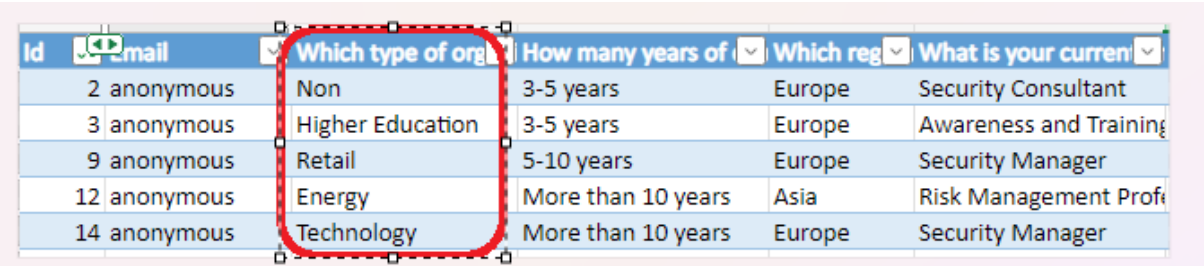
The final number of participants' data that meets the eligibility criteria is Twenty-four (24), ten (10) participants' data were disqualified due to the reasons mentioned above.

Figure 1: Exclusion based on years of experience



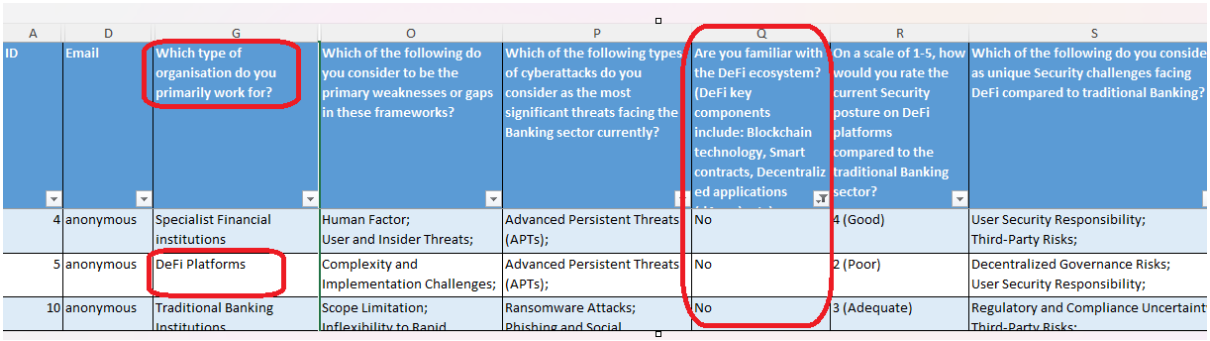
Id	Email	Which type of org	How many years of	Which reg	What is your curren
8	anonymous	Specialist Financial i	Less than 3 years	Europe	Security Auditor
15	anonymous	Regulatory and Sup	Less than 3 years	Europe	Security Consultant

Figure 2: Exclusion based on organisation/ sector



Id	Email	Which type of org	How many years of	Which reg	What is your curren
2	anonymous	Non	3-5 years	Europe	Security Consultant
3	anonymous	Higher Education	3-5 years	Europe	Awareness and Training
9	anonymous	Retail	5-10 years	Europe	Security Manager
12	anonymous	Energy	More than 10 years	Asia	Risk Management Profe
14	anonymous	Technology	More than 10 years	Europe	Security Manager

Figure 3: Exclusion based on lack of familiarity with DeFi



ID	Email	Which type of organisation do you primarily work for?	Which of the following do you consider to be the primary weaknesses or gaps in these frameworks?	Which of the following types of cyberattacks do you consider as the most significant threats facing the Banking sector currently?	Are you familiar with the DeFi ecosystem? (DeFi key components include: Blockchain technology, Smart contracts, Decentralized applications	On a scale of 1-5, how would you rate the current Security posture on DeFi platforms compared to the traditional Banking sector?	Which of the following do you consider as unique Security challenges facing DeFi compared to traditional Banking?
4	anonymous	Specialist Financial institutions	Human Factor; User and Insider Threats;	Advanced Persistent Threats (APTs);	No	4 (Good)	User Security Responsibility; Third-Party Risks;
5	anonymous	DeFi Platforms	Complexity and Implementation Challenges;	Advanced Persistent Threats (APTs);	No	2 (Poor)	Decentralized Governance Risks; User Security Responsibility;
10	anonymous	Traditional Banking Institutions	Scope Limitation; Inflexibility to Rapid	Ransomware Attacks; Phishing and Social	No	3 (Adequate)	Regulatory and Compliance Uncertaint Third-Party Risks:

Table 2: Disqualified participants with reasons.

Participant ID	Reasons for Disqualification	Provided Response
2	Non related financial sector experience, and Not familiar with DeFi	Non, No
3	Non related financial sector experience	Higher Education
4	Not familiar with DeFi	No
5	Not familiar with DeFi	No
8	Less than 3 years experience	Less than 3 years
9	Non related financial sector experience	Retail
10	Not familiar with DeFi	No
12	Non related financial sector experience	Energy
14	Non related financial sector experience	Technology
15	Less than 3 years experience, and Not familiar with DeFi	Less than 3 years, No

3.3.2. Statistical Techniques

The sample was divided into three groups based on years of experience: 3-5 years with a sample size of eight (8), 5-10 years with a sample size of thirteen (13), and the final group, 10 years plus, with a sample size of three (3). The average confidence across the three groups was 3.

To analyse the data, the descriptive statistical method was used to determine the average confidence of the participants in the effectiveness of the frameworks based on their experience with them. The standard deviation of the sample was also taken to establish the degree of variability within the group.

One-way ANOVA was used to analyse the sample to determine if there were statistically significant differences between the means of the three groups. This was done in an attempt to shed light on whether the variation in my data can be attributed to the differences in the years of experience by which the sample was separated into the three groups or if it is due to random variation within the groups. The 24 experienced participants all believed that cybersecurity frameworks are instrumental in securing the financial services sector, with a very popular indication for PCI-DSS, NIST frameworks and ISO27001/2 being the most popular among all.

Table 3: One way ANOVA result

Anova: Single Factor

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Group 1	8	24	3	0
Group 2	13	45	3.461538	0.269231
Group 3	3	11	3.666667	0.333333

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.435897	2	0.717949	3.868421	0.037127	3.4668
Within Groups	3.897436	21	0.185592			
Total	5.333333	23				

The results of the ANOVA shows that there is a statistically significant difference between the means of groups 1, 2, and 3 especially as the **P-value (0.037)** is less than the common alpha level of 0.05. It is however safe to conclude that at least one group's mean is significantly different from the others. This study will benefit from further analysis that would possibly help to determine exactly which groups differ from each other. Additionally, since the sample size is so small, this result may be misleading. The **F-statistic** is used to determine whether there is a statistically significant difference between the group means. From the results, the F-Statistic (3.87) which is the ratio of the variance between the groups to the variance within the groups, since the value of 3.87 is greater than the F critical value of 3.47, suggests that the variance between the group means is more than what would be expected due to random chance.

3.4. Ethical Considerations

The design of the survey was conducted with both professional and research ethics in mind, taking into account the General Data Protection Regulation (GDPR) to ensure that the rights of participants were not infringed upon. The survey provided participants with full information on the study's purpose and potential risks, allowing them to make an informed decision about their participation. The eligibility criteria and assumption that the respondents were to be over 18 years of age and must have experience in the financial sector were also clearly stated. The recruitment process and inclusion criteria were specified to ensure that only appropriate participants were included in the sample. The study employs a rigorous sampling strategy to guarantee that the results are representative of the target population and free from bias. The

inclusion criteria also ensure that the participants are representative of the population being studied, enhancing the generalizability of the results.

Sensitive information that could potentially identify any of the participants was not collected. All responses were obtained anonymously, which means that none of the information gathered can be used to identify any living individual. This approach ensures that the data collected is representative of the population as much as possible, without any biases or influences from identifiable individuals. Consequently, the results obtained from the data collection process will be unbiased and accurate, enabling a thorough understanding of the subject matter as much as is feasible with the available data.

The data collected were stored in a private OneDrive account that is accessible only to me. The OneDrive account is private, meaning that only authorized users are allowed access to the files and information stored in the account. The account is protected by Microsoft's default security, and no additional security measures are required as there are no confidential details held on the account. The data collected is solely for analysis and will be deleted once the project is completed.

3.5. Limitations

One of the limitations of this research is the methodology. The thesis employs the quantitative research methodology to understand what professionals think are effective and useful frameworks in securing the financial sector as well as what they think is applicable to the DeFi platforms in an attempt to secure those platforms, while these are all based on personal opinions which would have been influenced by a variety of factors, this study did not go further to understand the rationale behind such opinions, the why. Furthermore, to ensure the confidentiality of the data collected, the survey's design included a statement informing participants that their responses would be kept anonymous. Although the survey explored the willingness of participants to engage further with the research by checking their availability for interviews, the response was very poor; only 3 out of the 34 participants indicated their willingness to contribute further.

Another limitation of this research is the available data set for analysis. The survey instrument was shared with three different groups of over 400 cybersecurity professionals who are geographically dispersed across the globe; a paltry response of only 34 was received from the three groups. The population size of 400, which is the total of the three groups, is not an accurate reflection of cybersecurity professionals worldwide. This is a far cry from the ISC2 estimate of 5.5million in 2023 [100] and the total responses received from the three groups are less than 10%.

Chapter 4: Results, Discussions, and Recommendations.

The focus of this work is in two fold, the first been to assess the effectiveness of cybersecurity frameworks in the financial and banking sector, and the second is to assess if these frameworks can also be used in solving the issue of providing security to the nascent DeFi environment. An additional question or follow-up question from the possible adaptability of existing frameworks to DeFi is the question of whether there is a need for completely new sets of DeFi-focused frameworks. It has been established that cybersecurity frameworks are multidimensional in use and application, they are sometimes used for regulatory and mandatory compliance requirements e.g. PCI-DSS, GDPR or UK DPA, they can be used for establishing a baseline of security controls e.g., ISO27002 and NIST, with some others running certification programs, they also meet that need for certification e.g. the ISO27001 and many other reasons. For the purpose of this project I focused on the use of the framework as a tool for establishing a system of consistent and repeatable practices within individual organisations that enables them to manage risks to their information security data, systems and components and as a tool of compliance. The rest of this chapter will focus on the discussions of the results and the findings from the literature review from Chapter 2.

4.1. Are cybersecurity frameworks effective?

Are the existing cybersecurity frameworks effective in the mitigation of cyberattacks against the banking and financial sector? The literature review in Chapter 2 reveals that there is a consensus among the different works examined that the frameworks are essential and provide a system of basic foundational practices, opinions are divided on the level of effectiveness or adequacy of the frameworks, and some believe that as a starting point. They provide foundational and general best practices, some of the main arguments against these existing frameworks' effectiveness are that they are generalist in nature (meaning they are not specifically crafted for the sector), they are not dynamic and not very responsive to changes. Exploring whether practising cybersecurity professionals share a similar view as the findings from the literature, two questions in the survey were posed to participants to understand their opinion on this subject of effectiveness.

The first of the two questions is **question 5** which says: “Which Security or Regulatory Framework do you consider as effective in mitigating cyber-attacks within the Banking Sector? (Select all that apply)”, results to this question in **Column K** (table 4) reveal that almost all the valid participants identified ISO27001/2, PCI-DSS, and NIST as the top 3 frameworks, only one person did not mention all top three (3) frameworks. The other ones that were

mentioned were the NIS NIS2 and SOX regulations. The significance of this question is that there is a consensus with regards to which ones are the top frameworks in the industry (since the ones identified in the literature match almost perfectly with what my study reveals), this prepares a good case for establishing a basis of comparison between both information sources. The second question still on the topic of the effectiveness of frameworks was survey **question 7** which says: "On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in the traditional Banking sector?", results to this question in **Column M** (table 5) reveals that every one of the 24 participants believed that the frameworks were effective in mitigating cyberattacks, 16 participants (table 5) thinks that the frameworks are "moderately effective", while the remaining 8 participants (table 4) thinks they are "very effective". I also noticed that the 8 participants who think the frameworks were very effective all had a minimum of 5years of experience, 2 of the 8 participants had over 10 years of experience, it is not possible to ascertain how close the other 6 participants were to 10 years' experience, it would have been very beneficial to understand the reasons why these more experienced professionals think this framework is very effective, perhaps they have had experiences of the history of when there were no meaningful frameworks or no frameworks at all. It is also interesting that if these more experienced professionals, thinks these frameworks are "very effective" and the literature thinks they are not that effective, then there is a need for further research in this area. That said, my sample size is not large enough to be representative of the general population of experienced cybersecurity professionals. I believe future works that analyse cyberattacks in the banking sector by focusing on which frameworks are used, how they are used, what type of attack was suffered, and an end-to-end study of particular cyberattacks will help the understanding of whether these frameworks are effective or not, and to what extent were they in mitigating attacks.

Table 4:

A	G	H	K	M
)	Question 1: Which type of organisation do you primarily work for?	Question 2: How many years of experience do you have in Cybersecurity or related fields?	Question 5: Which Security or Regulatory Framework do you consider as effective in mitigating cyber-attacks within the Banking Sector? (Select all that apply).	Question 7: On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector?
1	Specialist Financial institutions	More than 10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; NIS and NIS 2;	4 (Very effective)
7	Financial Technology (FinTech) Comapnies	5-10 years	NIST Cybersecurity Framework (CSF) & SP 800 series; Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); Sarbanes-Oxley Act (SOX); European Payment Services Directive (PSD2);	4 (Very effective)
11	Financial Technology (FinTech) Comapnies	5-10 years	NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	4 (Very effective)
13	Financial Technology (FinTech) Comapnies	5-10 years	NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	4 (Very effective)
16	Digital and Online Banks	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	4 (Very effective)
17	Financial Technology (FinTech) Comapnies	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regularion (GDPR);	4 (Very effective)
18	Specialist Financial institutions	5-10 years	ISO 27000 Series; Payment Card Industry Data Security Standard (PCI DSS); NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	4 (Very effective)
22	Traditional Banking Institutions	More than 10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	4 (Very effective)

Table 5:

ID	Question 1: Which type of organisation do you primarily work for?	Question 2: How many years of experience do you have in Cybersecurity or related fields?	Question 5: Which Security or Regulatory Framework do you consider as effective in mitigating cyber-attacks within the Banking Sector? (Select all that apply).	Question 7: On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector?
6	Specialist Financial institutions	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regularion (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; NIS and NIS 2;	3 (Moderately effective)
19	Traditional Banking Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)
20	Digital and Online Banks	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)
21	Financial Technology (FinTech) Companies	More than 10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)
23	Specialist Financial institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; NIS and NIS2;	3 (Moderately effective)
24	Financial Technology (FinTech) Companies	5-10 years	ISO 27000 Series; Payment Card Industry Data Security Standard (PCI DSS); NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)
25	Financial Technology (FinTech) Companies	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)
26	Traditional Banking Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)
27	Traditional Banking Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)
28	Traditional Banking Institutions	5-10 years	ISO 27000 Series; Payment Card Industry Data Security Standard (PCI DSS); General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)
29	Financial Technology (FinTech) Companies	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)
30	Specialist Financial institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)
31	Digital and Online Banks	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)
32	Financial Technology (FinTech) Companies	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)
33	Traditional Banking Institutions	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)
34	Financial Technology (FinTech) Companies	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series;General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)

4.2. Are the frameworks applicable to DeFi?

In an attempt to answer this question, again using the Likert scale of 1 to 5 for the answers, two (2) questions were posed to the participants, the first question was to get an understanding of their perception of the current security posture of the DeFi platform and the second question was to explore their opinion on the applicability of existing cybersecurity frameworks to DeFi platforms. The first of these two questions which was **question number 12** asks "On a scale of 1-5, how would you rate the current Security posture on DeFi platforms compared to the traditional Banking sector?", answers are recorded in **Column R**. The question assumes that the participants were at the minimum familiar with DeFi platforms, these is the reason why respondents who were not familiar with DeFi platforms were removed at the data cleaning stage in chapter 3. The participants with a "maybe" answer were considered eligible with the assumption that have read the description of DeFi that was provided in the questions, they at least have 50% knowledge of what DeFi. Analysing the results, 6 of the 24 eligible participants thought that the security in DeFi platforms, there is a mixture of experiences among the 6 participants, what is immediately obvious was that the 6 participants also thinks that the cybersecurity frameworks were effective in mitigating cyberattacks in the response to **question 7 in column M.** Perhaps this participant works in organisations that have embraced DeFi, only one of the 6 participants indicated that they are currently employed in a traditional banking institution, the remaining 5 participants all work for either Fintech, Digital banks or Specialist institutions. Again the opportunity to gain further insight into the reasons behind the responses especially by this 6 participants was lost as this research did not proceed with an interview. The remaining 18 participants, were all of the opinion that security on DeFi platforms was either "poor" or "very poor".

Expert opinion from the literature review in chapter 2 indicates that there are major security challenges that has led to cyberattack assuming that cyberattacks are directly as a result of ineffective security controls. The survey result can be interpreted to agree with expert opinion as 75% (18 participants) where the eligible participants all concluded that security on DeFi compared to traditional banking and financial sector was either "poor" or "very poor". This research did not go further to explore what their rationale was for the answer choices, or which aspects of the cybersecurity programs in DeFi were poor. Although a follow-up question was posed to the participants and asked what they considered the most unique security challenges facing DeFi, the top answers were Decentralized Governance Risk, Regulatory and Compliance Uncertainty, Phishing and Social Engineering, and Third-Party Risks. It is also not very clear at this stage whether these responses were as a result of their own personal or

professional experiences, whether they have been influenced by things they have heard or read, or whether they have been following incidents and cyberattacks reporting online and in the media. The survey also did could not furnish information on what basis these participants made their comparisons. Again all of this other information could have been gathered qualitatively through an interview to gather those perspectives.

The second question which is the main question was question number 14 which asks: "Do you believe that existing Banking sector Cybersecurity and Regulatory Frameworks can be effectively applied to DeFi platforms?" results are in Column T. Only one of the 24 valid participants (P13) answered in the negative with a "no", 12 of the 24 participants (50%) answered with an affirmative "yes" and the remaining 11 participants answered with scepticism, "maybe". The result of the 11 participants that answered may be interesting, I noticed that these respondents all responded with "moderately effective" in **column M to question 7** on "How would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector?" except for one participant (P1) who thought the frameworks were already "very effective" in mitigating cyberattacks in traditional banking (**column M to question 7**), and that security posture in DeFi was "good" in response to question **(column R question 12),** this response maybe considered as an outlier. All other respondents in this group who answered "maybe" (**column T question 14**), thought that the frameworks were "moderately effective" (**column M to question 7**) and that security posture in DeFi was mostly "poor", only 2 participants (P20 and P27) thinks they were adequate **(column R question 12).**

It is also interesting to note that years of experience did not appear to have influenced the answer choices, there was also a mix in the type of institutions they worked for, but this does not appear to play any role in the answers.

The opinion of academia from the literature review in Chapter 2 on the potential applicability of existing Banking sector Cybersecurity frameworks to DeFi platforms is divided, some have argued that those frameworks are not even specific to the sector, with the argument that because frameworks such as ISO2700 and NIST are generally applicable in different sector makes it more unlikely unfit for application to DeFi sector. While the argument maybe correct, the advocates of this idea were not able to provide any cogent reason why they believe the argument generalisability of those frameworks is a reason for disqualification, after all, foundational or basic cybersecurity hygiene practices should be industry or sector-agnostic. Most of the scholars agreed that the frameworks are essential at least to the extent that it offer what has been referred to as basic or foundational control, it would be most helpful if it were

possible to pinpoint in what areas these frameworks are inadequate backed up by empirical data. Some others have proposed that the frameworks could be tweaked in order for it to be fit for purpose, others have outrightly suggesting new sets of regulations [101], as the current ones in use are only guidelines and non-mandatory, claiming that existing ones are not dynamic enough to adequately meet the ever changing complex DeFi environments. One the challenges against this idea is that it takes a long time to update frameworks, a good example is the PCI-DSS v3.2.1 which was recently retired on 31st March 2024, it was evident that it did not address new and emerging technologies such as cloud service, the need for an update became more evident the regulator commenced the review program in 2019. Timeline for review and development and adoption of the new version took around 4years [102]. The other challenge was the issue of the inconclusive meaning of decentralisation and the illusion that it creates. The sample results could be interpreted as matching the dichotomy that is evident in the literature findings. Opinions are divided, maybe not as clear cut as the responses to the survey questions but, it is evident that there is more that needs to be done in the area of research identified.

Table 6

A	G	H	M	R	T
ID	Question 1: Which type of organisation do you primarily work for?	Question 2: How many years of experience do you have in Cybersecurity or related fields?	Question 7: On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector?	Question 12: On a scale of 1-5, how would you rate the current Security posture on DeFi platforms compared to the traditional Banking sector?	Question 14: Do you believe that existing Banking sector Cybersecurity and Regulatory Frameworks can be effectively applied to DeFi platforms?
1	Specialist Financial institutions	More than 10 years	4 (Very effective)	4 (Good)	Maybe
6	Specialist Financial institutions	5-10 years	3 (Moderately effective)	2 (Poor)	Yes
7	Financial Technology (FinTech) Comapnies	5-10 years	4 (Very effective)	2 (Poor)	Yes
11	Financial Technology (FinTech) Comapnies	5-10 years	4 (Very effective)	2 (Poor)	Yes
13	Financial Technology (FinTech) Comapnies	5-10 years	4 (Very effective)	3 (Adequate)	No
16	Digital and Online Banks	5-10 years	4 (Very effective)	2 (Poor)	Yes
17	Financial Technology (FinTech) Comapnies	5-10 years	4 (Very effective)	2 (Poor)	Yes
18	Specialist Financial institutions	5-10 years	4 (Very effective)	2 (Poor)	Yes
19	Traditional Banking Institutions	3-5 years	3 (Moderately effective)	2 (Poor)	Maybe

20	Digital and Online Banks	5-10 years	3 (Moderately effective)	3 (Adequate)	Maybe
21	Financial Technology (FinTech) Companies	More than 10 years	3 (Moderately effective)	2 (Poor)	Maybe
22	Traditional Banking Institutions	More than 10 years	4 (Very effective)	2 (Poor)	Yes
23	Specialist Financial institutions	3-5 years	3 (Moderately effective)	2 (Poor)	Maybe
24	Financial Technology (FinTech) Companies	5-10 years	3 (Moderately effective)	2 (Poor)	Maybe
25	Financial Technology (FinTech) Companies	3-5 years	3 (Moderately effective)	1 (Very poor)	Yes
26	Traditional Banking Institutions	3-5 years	3 (Moderately effective)	2 (Poor)	Maybe
27	Traditional Banking Institutions	3-5 years	3 (Moderately effective)	3 (Adequate)	Maybe
28	Traditional Banking Institutions	5-10 years	3 (Moderately effective)	2 (Poor)	Maybe
28	Traditional Banking Institutions	5-10 years	3 (Moderately effective)	2 (Poor)	Maybe
29	Financial Technology (FinTech) Companies	5-10 years	3 (Moderately effective)	1 (Very poor)	Yes
30	Specialist Financial institutions	3-5 years	3 (Moderately effective)	2 (Poor)	Maybe
31	Digital and Online Banks	5-10 years	3 (Moderately effective)	2 (Poor)	Maybe
32	Financial Technology (FinTech) Companies	3-5 years	3 (Moderately effective)	3 (Adequate)	Yes
33	Traditional Banking Institutions	5-10 years	3 (Moderately effective)	2 (Poor)	Yes
34	Financial Technology (FinTech) Companies	3-5 years	3 (Moderately effective)	3 (Adequate)	Yes

4.3. Are new frameworks for DeFi necessary?

To analyse this question for the opinion of the eligible 24 participants on the question of whether new frameworks were necessary, survey question number 17 was posed to them which asks: “On a scale of 1-5, how optimistic are you about the future of Security of DeFi platforms if traditional Banking Cybersecurity and Regulatory Frameworks were adopted?” result is in column W. From the results, 19 of the eligible participants were optimistic with a “moderately optimistic” response and a further 4 participants (P7, P19, P31, P34) were “very optimistic”, one participant (P1) was “extremely optimistic”. Statistically, the average response of all the participants indicated optimism which is a good indication signalling hope for the future.

On the question of whether there is a need for new sets of from works, question 18 was posed to participants asking: “Do you see a need for entirely new frameworks to address the unique aspects of DeFi?” results in column Y, only one participant (P11) thought there was no need for new frameworks, all other 23 participants answered in the affirmative that there was a new framework for the DeFi environment.

The literature review highlighted the need for regulatory frameworks because there is an absence of consistent and unified regulations across different jurisdictions, i.e., regulatory ambiguity. From the review, there are no global DeFi regulations, rather international organisations such as the IMF [33] are calling for national governments to create national regulations for their jurisdictions, but the academic research community on the other hand advocating for working together between regulators, industry participants, policymakers, and other stakeholders so as to develop balanced regulatory frameworks that remove uncertainty and ambiguity in DeFi environment [101].

4.4. Recommendations

Despite many of the researchers calling for updates or changes to existing frameworks, the process of changing or updating frameworks takes time and a lot of manpower and resources. For example, it took 4 years to update PCI-DSS v3.2.1 to v4.0, from 2019 [102], ISO27001 the 2013 version did not get updated until nine (9) years later in 2022, in 2024, NIST recently released version 2.0 of the NIST CSF.

Baseline security is fundamental and should not be drastically different in implementation from sector to sector, I believe the existing frameworks can initially provide the necessary basic security that is lacking in DeFi, and most importantly there is an urgent need for more understanding about DeFi and its various implementations. A framework like PCI-DSS that is focused on DeFi could work, but this is suggestive that an organisation or some stakeholders will come together like the founding members did in PCI-DSS to form the PCI SSC and then make the regulations that all participating organisations have to comply with. If this idea is taken it means that whatever amount of decentralisation currently exists will have to be given up to such groups of stakeholders to make rules for all participants. There lies the conundrum. Assuming that Decentralisation does exist in DeFi, how much of it are we willing to give up for the type of security we desire?

Chapter 5: Conclusion

5.1. Conclusion

This dissertation started to achieve 3 main objectives, namely (1) to assess the effectiveness of existing cybersecurity frameworks in the traditional banking and financial sector, (2) to assess the potential applicability of those frameworks to the DeFi environment and (3) to assess whether there is a need for new sets of frameworks for the DeFi environment.

Despite the popularity of some of the frameworks that are in common use in the sector across the world, through this research, I have been able to establish that professionals are not very confident about the effectiveness or adequacy of these frameworks. Literature review revealed some of the downfalls of the frameworks including the generalisability of the frameworks and their supposed lack of regular updates to keep up with dynamic and complications that comes with technological advancements. The effectiveness of the frameworks in mitigating cyberattacks was a challenge as there were no empirical data or end-to-end case studies that could have been analysed to establish how reliable those frameworks have been.

On the question of whether those frameworks could be effective in mitigating cyberattacks in the DeFi environment, from the available literature and findings from my survey, opinions are currently divided with the majority advocating for new frameworks that are DeFi-focused. And this seems like a reasonable conclusion, individual countries are making efforts within their borders to deal with the challenges from a legal perspective. This current lack of congruence between the approaches different countries of the world have adopted in recognition of and responding to threats posed by crypto assets. Some countries have developed frameworks for dealing with the risks e.g. UK through the Financial Conduct Authority (FCA) and Financial Services and Markets Act 2000 has promulgated several regulations such as the requirement for every crypto exchange or custodian wallet provider to be registered under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) [103]. Some countries like India have no laws or regulations prohibiting activities in crypto assets, anyone holding crypto assets does so at their own risk as it is currently unregulated [104], in countries like Nigeria, crypto is not recognised as a legal tender, hence unregulated [105], in the US, crypto assets are not legal tenders but they are recognised and regulated to an extent by existing regulations such as the Bank Secrecy Act and the USA Patriot Act, Commodity Exchange Act etc., [106], in China crypto assets and related activities are banned and illegal but blockchain technology without the currency is supported and encouraged [107].

Despite the varying approaches taken by countries, it is clear that the regulation of crypto assets is a complex issue that requires careful consideration and attention from governments and regulatory bodies. DeFi, Blockchain, Decentralised Ledger, Cryptocurrency, all these technologies need to be properly understood to be able to make meaning regulation that would not inadvertently create further vulnerabilities that could be exploited by cybercriminals.

5.2. Further Research

This dissertation aims to study the effectiveness of the cybersecurity frameworks in mitigating cyberattacks in the banking sector and its potential applicability to DeFi environments uncovering some areas of research that need further investigation. The points raised by the academic research on the adequacy of the frameworks in themselves as a tool for mitigating cyberattacks in traditional banking and financial sector is largely that it is mostly not specific to the industry, this may be a valid point but I feel it is not enough to condemn those frameworks. Recent studies highlight significant gaps in cybersecurity frameworks for the banking and financial sector. While frameworks like NIST provide guidelines, their voluntary nature and lack of legal mandates limit their effectiveness [37]. Whether it mitigates cyberattacks or not, more research is needed in this area and a system/strategy needs to be developed to measure the effectiveness of cyberattacks. The major challenge with this suggestion is that cyberattack investigation usually involves professionals across multiple sectors, it takes a long time between knowing of the attack and reaching a conclusion on how the breach happened and what aspects were involved or even when the attack started, in some real-life examples the breach was not noticed until when the attack materialised, most times the breach would have happened several months earlier. The same unfortunately applies to the DeFi environment. Empirical data on the relationships between cyberattacks or cyber-incidents /events and how cybersecurity frameworks were instrumental in the attack mitigation will offer more benefits.

Other areas that could benefit from future research in information sharing, aside from the data breaches reporting for GDPR and DPA, and those done as part of incident reporting, there are no other mandatory reporting for incidents and events, there may be a possibility of under-reporting going on in areas where there are no strict reporting requirements. Research indicates a disparity between the sophistication of cyber threats and current security measures [96], [108]. The need for more adaptable, robust, and technology-driven frameworks is

emphasised [108], with recommendations for integrating advanced technologies like AI and Big Data analytics [108], [109].

Appendices

Appendix A: Data Collection Survey

Can%20Regulatory
%20Frameworks%20

Can Regulatory Frameworks Improve the Mitigation of Cyberattacks in Decentralized Finance?

I am Yomi Olutimehin, an MSc Information Security student at Royal Holloway University of London (RHUL).

I am researching the topic: "**Assessing the Effectiveness of Regulatory Frameworks in Mitigating Cyber Attacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi)".**
This study aims to assess the effectiveness of Security Frameworks in mitigating cyber-attacks within the Banking sector and to explore their applicability to decentralized finance (DeFi).

In compliance with the General Data Protection Act 2018, your invaluable responses which are collected anonymously for research analysis will be kept strictly confidential. Responses cannot be traced back to respondents, neither can any of the responses be used to identify them.

You are at liberty to discontinue the questionnaire at any time, your responses will not be saved until you submit them. If after submission you change your mind, your response which would have been included in the study will be irretrievable. As it will not be possible to identify which submission was yours, I request that you think about it before submitting the questionnaire.

If you select the option to participate in further study, you will be contacted via provided details which will be treated confidentially.

Eligibility for your data to be included in the study are:
*If you are a cybersecurity professional
*over the age of 18 years
*Experience within the Financial Sector or Financial Technology organisation.

* Required

Demographic Information

1. Which type of organisation do you primarily work for? *

- ◯ Traditional Banking Institutions
- ◯ Specialist Financial institutions
- ◯ Digital and Online Banks
- ◯ Financial Technology (FinTech) Companies
- ◯ DeFi Platforms
- ◯ Regulatory and Support institutions
- ◯ Other

2. How many years of experience do you have in Cybersecurity or related fields? *

- ◯ Less than 3 years
- ◯ 3-5 years
- ◯ 5-10 years
- ◯ More than 10 years

3. Which region do you primarily work in? *

- ◯ North America
- ◯ Europe
- ◯ Asia
- ◯ South America
- ◯ Africa
- ◯ Australia

4. What is your current professional role? *

- ◯ Chief Information Security Officer (CISO)
- ◯ Security Manager
- ◯ Security Architect
- ◯ Security Consultant
- ◯ Blockchain Developer
- ◯ Compliance Manager
- ◯ Security Auditor
- ◯ Risk Management Professional
- ◯ Other

Security Frameworks in Traditional Banking

5. Which Security or Regulatory Framework do you consider as effective in mitigating cyberattacks within the Banking Sector? (Select all that apply). *

- [ ] Payment Card Industry Data Security Standard (PCI DSS)
- [ ] ISO 27000 Series
- [ ] General Data Protection Regulation (GDPR)
- [ ] NIST Cybersecurity Framework (CSF) & SP 800 series
- [ ] Basel III
- [ ] NIS and NIS2
- [ ] Sarbanes-Oxley Act (SOX)
- [ ] European Payment Services Directive (PSD2)
- [ ] Other

6. On a scale of 1-5, how effective are these frameworks implemented in your organisation? *

- ○ 1 (Not at all effective)
- ○ 2 (Slightly effective)
- ○ 3 (Moderately effective)
- ○ 4 (Very effective)
- ○ 5 (Extremely effective)

7. On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector? *

- ○ 1 (Not effective)
- ○ 2 (Neither effective nor ineffective)
- ○ 3 (Moderately effective)
- ○ 4 (Very effective)
- ○ 5 (Extremely effective)

8. Which of the following do you consider to be the main strengths of current Security Frameworks in the Banking sector? Select all that apply. *

- ☐ Comprehensive Security Controls
- ☐ Risk-Based Approach
- ☐ Continuous Monitoring and Incident Management
- ☐ Strong Data Protection and Encryption
- ☐ Audit and Compliance Measures
- ☐ Third-Party Management
- ☐ User Awareness and Training

9. Which of the following do you consider to be the primary weaknesses or gaps in these frameworks? *

- [ ] Complexity and Implementation Challenges
- [ ] Static Nature of Compliance
- [ ] Scope Limitation
- [ ] Inflexibility to Rapid Technology
- [ ] User and Insider Threats
- [ ] Human Factor
- [ ] Metrics and Measurement

10. Which of the following types of cyberattacks do you consider as the most significant threats facing the Banking sector currently? *

- [ ] Ransomware Attacks
- [ ] Phishing and Social Engineering Attacks
- [ ] Advanced Persistent Threats (APTs)
- [ ] Insider Threats
- [ ] Credential Stuffing
- [ ] Malware and Banking Trojans
- [ ] Supply-Chain Attacks
- [ ] Distributed Denial of Service (DDoS)
- [ ] Account Takeover

Decentralized Finance (DeFi) Security

11. Are you familiar with the DeFi ecosystem? (DeFi key components include: Blockchain technology, Smart contracts, Decentralized applications (dApps), etc) *

- ◯ Yes
- ◯ No
- ◯ Maybe

12. On a scale of 1-5, how would you rate the current Security posture on DeFi platforms compared to the traditional Banking sector? *

- ◯ 1 (Very poor)
- ◯ 2 (Poor)
- ◯ 3 (Adequate)
- ◯ 4 (Good)
- ◯ 5 (Very good)

13. Which of the following do you consider as unique Security challenges facing DeFi compared to traditional Banking? *

Please select at most 5 options.

- [ ] Smart Contract Vulnerabilities
- [ ] Decentralized Governance Risks
- [ ] Oracle Manipulation
- [ ] Regulatory and Compliance Uncertainty
- [ ] User Security Responsibility
- [ ] Legacy Systems
- [ ] Scalable and Network Congestion
- [ ] Insider Threats
- [ ] Phishing and Social Engineering
- [ ] Liquidity Risks
- [ ] Third-Party Risks
- [ ] Advanced Persistent Threats (APTs)

14. Do you believe that existing Banking sector Cybersecurity and Regulatory Frameworks can be effectively applied to DeFi platforms? *

- ○ Yes
- ○ No
- ○ Maybe

15. On a scale of 1-5, how effective do you believe these adopted Frameworks could be in mitigating cyber-attacks in DeFi? *

- ○ 1 (Not effective)
- ○ 2 (Slightly effective)
- ○ 3 (Moderately effective)
- ○ 4 (Very effective)
- ○ 5 (Extremely effective)

16. What do you think are likely to be the main challenges in applying traditional banking sector Security Frameworks to DeFi platforms? *

- ☐ Decentralization (lack of Central authority)
- ☐ Pseudonymity and anonymity of users
- ☐ Resistance from DeFi community
- ☐ Complexity of Blockchain Technology
- ☐ Regulatory Uncertainty and Compliance
- ☐ Evolving Landscape and Innovation
- ☐ Artificial Intelligence and Machine Learning
- ☐ Other

17. On a scale of 1-5, how optimistic are you about the future of Security of DeFi platforms if traditional Banking Cybersecurity and Regulatory Frameworks were adopted? *

- ○ 1 (Not optimistic)
- ○ 2 (Slightly optimistic)
- ○ 3 (Moderately optimistic)
- ○ 4 (Very optimistic)
- ○ 5 (Extremely optimistic)

18. Do you see a need for entirely new frameworks to address the unique aspects of DeFi? *

- ○ Yes
- ○ No

19. Would you be willing to participate in further research on this topic? *

- ○ Yes
- ○ No

20. What is your email address? *

Appendix B: Valid /Eligible Data

ID	Question 1: Which type of organization do you primarily work for?	Question 2: How many years of experience do you have in Cybersecurity or related fields?	Question 5: Which Security or Regulatory Framework do you consider as effective in mitigating cyber-attacks within the Banking Sector? (Select all that apply).	Question 6: On a scale of 1-5, how effective are these frameworks implemented in your organization?	Question 7: On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector?	Question 12: On a scale of 1-5, how would you rate the current Security posture on DeFi platforms compared to the traditional Banking sector?	Question 14: Do you believe that existing Banking sector Cybersecurity and Regulatory Frameworks can be effectively applied to DeFi platforms?	Question 15: On a scale of 1-5, how effective do you believe these adopted Frameworks could be in mitigating cyber-attacks in DeFi?	Question 17: On a scale of 1-5, how optimistic are you about the future of Security of DeFi platforms if traditional Banking Cybersecurity and Regulatory Frameworks were adopted?	Lowest of the values in Column U and Column V	Question 18: Do you see a need for entirely new frameworks to address the unique aspects of DeFi?
1	Specialist Financial Institutions	More than 10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; NIS and NIS 2;	3 (Moderately effective)	4 (Very effective)	4 (Good)	Maybe	3 (Moderately effective)	5 (Extremely optimistic)	3	Yes
6	Specialist Financial Institutions	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; NIS and NIS 2;	4 (Very effective)	3 (Moderately effective)	2 (Poor)	Yes	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
7	Financial Technology (FinTech) Companies	5-10 years	NIST Cybersecurity Framework (CSF) & SP 800 series; Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); Sarbanes-Oxley Act (SOX); European Payment Services Directive (PSD2);	2 (Slightly effective)	4 (Very effective)	2 (Poor)	Yes	4 (Very effective)	4 (Very optimistic)	4	Yes
11	Financial Technology (FinTech) Companies	5-10 years	NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	4 (Very effective)	4 (Very effective)	2 (Poor)	Yes	4 (Very effective)	3 (Moderately optimistic)	3	No
13	Financial Technology (FinTech) Companies	5-10 years	NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)	4 (Very effective)	3 (Adequate)	No	3 (Moderately effective)	3 (Moderately optimistic)	3	No
16	Digital and Online Banks	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)	4 (Very effective)	2 (Poor)	Yes	4 (Very effective)	3 (Moderately optimistic)	3	Yes
17	Financial Technology (FinTech) Companies	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	4 (Very effective)	4 (Very effective)	2 (Poor)	Yes	4 (Very effective)	3 (Moderately optimistic)	3	Yes
18	Specialist Financial Institutions	5-10 years	ISO 27000 Series; Payment Card Industry Data Security Standard (PCI DSS); NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	4 (Very effective)	4 (Very effective)	2 (Poor)	Yes	4 (Very effective)	3 (Moderately optimistic)	3	Yes
19	Traditional Banking Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Maybe	4 (Very effective)	4 (Very optimistic)	4	Yes
20	Digital and Online Banks	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)	3 (Moderately effective)	3 (Adequate)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
21	Financial Technology (FinTech) Companies	More than 10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
22	Traditional Banking Institutions	More than 10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	4 (Very effective)	4 (Very effective)	2 (Poor)	Yes	4 (Very effective)	3 (Moderately optimistic)	3	Yes

ID	Question 1: Which type of organization do you primarily work for?	Question 2: How many years of experience do you have in Cybersecurity or related fields?	Question 5: Which Security or Regulatory Framework do you consider as effective in mitigating cyber-attacks within the Banking Sector? (Select all that apply).	Question 6: On a scale of 1-5, how effective are these frameworks implemented in your organization?	Question 7: On a scale of 1-5, how would you rate the overall effectiveness of these Frameworks in mitigating cyber-attacks in traditional Banking sector?	Question 12: On a scale of 1-5, how would you rate the current Security posture on DeFi platforms compared to the traditional Banking sector?	Question 14: Do you believe that existing Banking sector Cybersecurity and Regulatory Frameworks can be effectively applied to DeFi platforms?	Question 15: On a scale of 1-5, how effective do you believe these adopted Frameworks could be in mitigating cyber-attacks in DeFi?	Question 17: On a scale of 1-5, how optimistic are you about the future of Security of DeFi platforms if traditional Banking Cybersecurity and Regulatory Frameworks were adopted?	Loweset of the values in Column U and Column W	Question 18: Do you see a need for entirely new frameworks to address the unique aspects of DeFi?
			General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;								
23	Specialist Financial Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; NIS and MS2;	4 (Very effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
24	Financial Technology (FinTech) Companies	5-10 years	ISO 27000 Series; Payment Card Industry Data Security Standard (PCI DSS); NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
25	Financial Technology (FinTech) Companies	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)	3 (Moderately effective)	1 (Very poor)	Yes	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
26	Traditional Banking Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	4 (Very effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
27	Traditional Banking Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)	3 (Moderately effective)	3 (Adequate)	Maybe	4 (Very effective)	3 (Moderately optimistic)	3	Yes
28	Traditional Banking Institutions	5-10 years	ISO 27000 Series; Payment Card Industry Data Security Standard (PCI DSS); General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
29	Financial Technology (FinTech) Companies	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)	3 (Moderately effective)	1 (Very poor)	Yes	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
30	Specialist Financial Institutions	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; General Data Protection Regulation (GDPR);	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
31	Digital and Online Banks	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Maybe	3 (Moderately effective)	4 (Very optimistic)	3	Yes
32	Financial Technology (FinTech) Companies	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)	3 (Moderately effective)	3 (Adequate)	Yes	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
33	Traditional Banking Institutions	5-10 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series; General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series;	3 (Moderately effective)	3 (Moderately effective)	2 (Poor)	Yes	3 (Moderately effective)	3 (Moderately optimistic)	3	Yes
34	Financial Technology (FinTech) Companies	3-5 years	Payment Card Industry Data Security Standard (PCI DSS); ISO 27000 Series;General Data Protection Regulation (GDPR); NIST Cybersecurity Framework (CSF) & SP 800 series; Sarbanes-Oxley Act (SOX);	3 (Moderately effective)	3 (Moderately effective)	3 (Adequate)	Yes	4 (Very effective)	4 (Very optimistic)	4	Yes

Appendix C: Results in Columns

	A	B	C	D	E
1	Participant ID	Column M	Column R	Column U	Column W
2	1	4	4	3	5
3	6	3	2	3	3
4	7	4	2	4	4
5	11	4	2	4	3
6	13	4	3	3	3
7	16	4	2	4	3
8	17	4	2	4	3
9	18	4	2	4	3
10	19	3	2	4	4
11	20	3	3	3	3
12	21	3	2	3	3
13	22	4	2	4	3
14	23	3	2	3	3
15	24	3	2	3	3
16	25	3	1	3	3
17	26	3	2	3	3
18	27	3	3	4	3
19	28	3	2	3	3
20	29	3	1	3	3
21	30	3	2	3	3
22	31	3	2	3	4
23	32	3	3	3	3
24	33	3	2	3	3
25	34	3	3	4	4
26	Averages	3.333333333	2.208333333	3.375	3.25
27					

Appendix D: Statistical variation between groups

	A	B	C	D
	Participants	Group 1	Group 2	Group 3
		3	3	4
		3	4	3
		3	4	4
		3	4	
		3	4	
		3	4	
		3	4	
		3	3	
			3	
			3	
			3	
			3	
			3	
	Mean	3	3.461538462	3.666666667
	Median	3	3	4
	Standard Deviation	0	0.518874522	0.577350269

Frameworrks Comparison.xlsx

Research Questionnaire.xlsx

Bibliography

[1] ‘Glossary | CSRC’. Accessed: Aug. 24, 2024. [Online]. Available: https://csrc.nist.gov/glossary/

[2] ‘Total Value Locked (TVL) - Techopedia’. Accessed: Aug. 19, 2024. [Online]. Available: https://www.techopedia.com/definition/total-value-locked-tvl

[3] M. R. Randazzo, M. Keeney, E. Kowalski, D. M. Cappelli, and A. Moore, ‘Insider Threat Study: Illicit Cyber Activity in the Banking and Financ e Sector’.

[4] M. Wazid, S. Zeadally, and A. K. Das, ‘Mobile Banking: Evolution and Threats: Malware Threats and Security So lutions’, *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56–60, doi: 10.1109/mce.2018.2881291.

[5] O. Akinbowale, H. E. Klingelhöfer, and M. Zerihun, ‘Analysis of cyber-crime effects on the banking sector using the balanc ed score card: a survey of literature’.

[6] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, M. Alanazi, and S. A. Ebad, ‘Cyber Threats Classifications and Countermeasures in Banking and Financial Sector’, doi: 10.1109/ACCESS.2017.Doi.

[7] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, ‘Decentralized finance’, *Journal of Financial Regulation*, vol. 6, no. 2, pp. 172–203, Sep. 2020, doi: 10.1093/jfr/fjaa010.

[8] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, ‘Decentralized Finance (DeFi)’, *Journal of Financial Regulation*, vol. 6, no. 2, pp. 172–203, Sep. 2020, doi: 10.1093/jfr/fjaa010.

[9] P. K. Ozili, ‘Decentralized finance research and developments around the world’, *Journal of Banking and Financial Technology*, vol. 6, no. 2, pp. 117–133, 2022.

[10] A. Walch, ‘Deconstructing “Decentralization”: Exploring the Core Claim of Crypto Systems’. [Online]. Available: https://twitter.com/neha/status/1007579383417188353.

[11] S. Kaur, S. Singh, S. Gupta, and S. Wats, ‘Risk analysis in decentralized finance (DeFi): a fuzzy-AHP approach’, *Risk Management*, vol. 25, no. 2, Jun. 2023, doi: 10.1057/s41283-023-00118-0.

[12] L. Zhou *et al.*, ‘SoK: Decentralized Finance (DeFi) Attacks’, in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 2444–2461. doi: 10.1109/SP46215.2023.10179435.

[13] T. Oluwaseun Abrahams, S. Kuzankah Ewuga, S. Onimisi Dawodu, A. Oluwatoyin Adegbite, A. Olanipekun Hassan, and C. Author, ‘A REVIEW OF

CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION', *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 1–25, 2024, doi: 10.51594/csitrj.v5i.699.

[14] 'ISO/IEC 27001:2022 - Information security management systems — Requirements'. Accessed: Aug. 13, 2024. [Online]. Available: https://www.iso.org/standard/27001

[15] 'Cybersecurity Framework | NIST'. Accessed: Aug. 13, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[16] 'Official PCI Security Standards Council Site - Document'. Accessed: Aug. 13, 2024. [Online]. Available: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

[17] 'HIPAA Compliance and Enforcement | HHS.gov'. Accessed: Aug. 13, 2024. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

[18] 'Chapter 2 – Principles - General Data Protection Regulation (GDPR)'. Accessed: Aug. 13, 2024. [Online]. Available: https://gdpr-info.eu/chapter-2/

[19] 'Data protection: The Data Protection Act - GOV.UK'. Accessed: Aug. 13, 2024. [Online]. Available: https://www.gov.uk/data-protection

[20] 'The Sarbanes Oxley Act'. Accessed: Aug. 13, 2024. [Online]. Available: https://sarbanes-oxley-act.com/

[21] A. Zimba, 'A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks', *International Journal of Computer Network and Information Security*, vol. 14, no. 1, pp. 25–39, Feb. 2022, doi: 10.5815/ijcnis.2022.01.03.

[22] O. Gulyas and G. Kiss, 'Cybersecurity threats in the banking sector', *International Conference on Control, Decision and Information Technolo gies*.

[23] 'The 6 Biggest Cyber Threats for Financial Services in 2024 | UpGuard'. Accessed: Aug. 13, 2024. [Online]. Available: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

[24] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, 'Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature', Oct. 25, 2020, *Emerald Group Holdings Ltd.* doi: 10.1108/JFC-03-2020-0037.

[25] A. Abdajabar and N. A. Md Yunus, 'A REVIEW ON THE IMPACT OF CYBERSECURITY CRIMES IN FINANCIAL INSTITUTIONS DURING

THE TIME OF COVID-19', *Acta Informatica Malaysia*, vol. 7, no. 1, pp. 19–23, 2023, doi: 10.26480/aim.01.2023.19.23.

[26] 'GLOBAL FINANCIAL STABILITY REPORT APR INTERNATIONAL MONETARY FUND'. Accessed: Aug. 13, 2024. [Online]. Available: https://www.imf.org/en/Publications/GFSR

[27] 'Improving Fraud Detection in Banking Systems: RPA and Advanced Analytics Strategies'.

[28] A. Bouveret, *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund, 2018.

[29] J. Korte, 'Papers Mitigating cyber risks through information sharing', Henry Stewart Publications, 2017.

[30] O. Efijemue, E. Taiwo, O. Paul, and I. Ejimofor, 'Cybersecurity Strategies for Safeguarding Customer's data and Preventing Financial Fraud in the United States Financial Sectors'. [Online]. Available: https://www.researchgate.net/publication/372135342

[31] 'German banking IT company hit by DDoS attack - FStech Financial Sector Technology'. Accessed: Aug. 14, 2024. [Online]. Available: https://www.fstech.co.uk/fst/German_Banking_IT_Company_Hit_By_DDoS_Attack.php

[32] 'Timeline of Cyber Incidents Involving Financial Institutions - Carnegie Europe'. Accessed: Aug. 14, 2024. [Online]. Available: https://carnegieendowment.org/features/fincyber-timeline?lang=en&center=europe

[33] 'Cyberattacks threaten global financial stability, IMF warns | World Economic Forum'. Accessed: Aug. 15, 2024. [Online]. Available: https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

[34] Chandra sekhar and M. Kumar, 'An Overview of Cyber Security in Digital Banking Sector', *East Asian Journal of Multidisciplinary Research*, vol. 2, no. 1, pp. 43–52, Jan. 2023, doi: 10.55927/eajmr.v2i1.1671.

[35] P. C. Jacobs, S. H. Von Solms, and M. M. Grobler, 'Towards a framework for the development of business cybersecurity capabilities', 2016.

[36] 'Risk management - NCSC.GOV.UK'. Accessed: Aug. 17, 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/10-steps/risk-management

[37] S. Goodwin, 'The need for a financial sector legal standard to support the NIST Cybersecurity Framework', in *Conference Proceedings - IEEE*

SOUTHEASTCON, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 89–95. doi: 10.1109/SoutheastCon48659.2022.9764006.

[38] C. Calliess and A. Baumgarten, 'Cybersecurity in the EU the example of the financial sector: A legal perspective', 2020, *Cambridge University Press*. doi: 10.1017/glj.2020.67.

[39] 'Cybersecurity: Risks and management of risks for global banks and financial institutions Mark Camillo', 1752.

[40] F. Cremer *et al.*, 'Cyber risk and cybersecurity: a systematic review of data availability', *Geneva Papers on Risk and Insurance: Issues and Practice*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[41] 'National Cyber Strategy 2022 (HTML) - GOV.UK'. Accessed: Aug. 17, 2024. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[42] S. Al-Bassam and A. Al-Alawi, 'The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector', *Journal of Xidian University*, vol. 14, no. 7, Jul. 2019, doi: 10.37896/jxu14.7/174.

[43] A. Brilingaite, L. Bukauskas, A. Juozapavičius, and E. Kutka, 'Overcoming information-sharing challenges in cyber defence exercises', *J Cybersecur*, vol. 8, no. 1, 2022, doi: 10.1093/cybsec/tyac001.

[44] 'Organisations must do more to combat the growing threat of cyber attacks | ICO'. Accessed: Aug. 26, 2024. [Online]. Available: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/05/organisations-must-do-more-to-combat-the-growing-threat-of-cyber-attacks/

[45] D. Sulistyowati, F. Handayani, and Y. Suryanto, 'Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS', *JOIV : International Journal on Informatics Visualization*, vol. 4, no. 4, pp. 225–230, Dec. 2020, doi: 10.30630/joiv.4.4.482.

[46] S. Onimisi Dawodu, A. Omotosho, O. Josephine Akindote, A. Oluwatoyin Adegbite, S. Kuzankah Ewuga, and C. Author, 'CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES', *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 220–243, 2023, doi: 10.51594/csitrj.v659.

[47] Abimbola Oluwatoyin Adegbite, Deborah Idowu Akinwolemiwa, Prisca Ugomma Uwaoma, Simon Kaggwa, Odunayo Josephine Akindote, and Samuel Onimisi Dawodu, 'REVIEW OF CYBERSECURITY STRATEGIES IN PROTECTING NATIONAL INFRASTRUCTURE: PERSPECTIVES FROM

THE USA', *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 200–219, Dec. 2023, doi: 10.51594/csitrj.v4i3.658.

[48] 'The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022'. Accessed: Aug. 24, 2024. [Online]. Available: https://www.legislation.gov.uk/uksi/2022/860/contents/made

[49] 'CBEST Threat Intelligence-Led Assessments | Bank of England'. Accessed: Aug. 24, 2024. [Online]. Available: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide

[50] 'Operational resilience of the financial sector | Bank of England'. Accessed: Aug. 24, 2024. [Online]. Available: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector

[51] D. Mohammed, M. Omar, and V. Nguyen, 'Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards', 2017, pp. 113–129. doi: 10.4018/978-1-5225-0741-3.ch005.

[52] Onyeka Chrisanctus Ofodile *et al.*, 'DIGITAL BANKING REGULATIONS: A COMPARATIVE REVIEW BETWEEN NIGERIA AND THE USA', *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 347–371, Mar. 2024, doi: 10.51594/farj.v6i3.897.

[53] N. S. Uzougbo, C. G. Ikegwu, and A. O. Adewusi, 'Cybersecurity compliance in financial institutions: a comparative analysis of global standards and regulations', *International Journal of Science and Research Archive*, vol. 12, no. 1, pp. 533–548, 2024.

[54] A. Oyewole, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu, 'Cybersecurity risks in online banking: A detailed review and preventiv e strategies applicatio', *World Journal of Advanced Research and Reviews*.

[55] 'PCI Merchant Levels 1 - 4 for VISA and Mastercard for SAQ and Level 1'. Accessed: Aug. 14, 2024. [Online]. Available: https://pcipolicyportal.com/what-is-pci/merchants/

[56] 'CMMI Institute - CMMI Levels of Capability and Performance'. Accessed: Aug. 14, 2024. [Online]. Available: https://cmmiinstitute.com/learning/appraisals/levels

[57] 'Incident management - NCSC.GOV.UK'. Accessed: Aug. 14, 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/10-steps/incident-management

[58] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, 'SoK: Decentralized Finance (DeFi)', *Conference on Advances in Financial Technologies*.

[59] F. Carapella, E. Dumas, J. Gerszten, N. Swem, and L. Wall, ‘Decentralized Finance (DeFi): Transformative Potential & Associate d Risks’, *Finance and Economics Discussion Series*, vol. 2022, no. 057, pp. 1–33, doi: 10.17016/feds.2022.057.

[60] P. Schueffel, ‘DeFi: Decentralized Finance - An Introduction and Overview’, *Journal of Innovation Management*, vol. 9, no. 3, pp. I–XI, doi: 10.24840/2183-0606_009.003_0001.

[61] U. W. Chohan, ‘Decentralized Finance (DeFi): An Emergent Alternative Financial Archit ecture’, *Social Science Research Network*.

[62] T. Yuyama, K. Katayama, and P. Brigner, ‘Proposal of Principles of DeFi Disclosure and Regulation’, *FC Workshops*.

[63] J. R. Jensen, V. von Wachter, and O. Ross, ‘An Introduction to Decentralized Finance (DeFi)’, *Complex Systems Informatics and Modeling Quarterly*.

[64] ‘Crypto regulatory affairs: Swiss regulator publishes guidance for stablecoin issuers and banks offering guarantees’. Accessed: Aug. 13, 2024. [Online]. Available: https://www.elliptic.co/blog/crypto-regulatory-affairs-swiss-regulator-publishes-guidance-for-stablecoin-issuers-banks-offering-guarantees

[65] F. Schär, ‘Decentralized finance: on blockchain-and smart contract-based financial markets’, *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021, doi: 10.20955/r.103.153-74.

[66] B. Kaplan, V. F. Benli, and E. A. Alp, ‘Decentralize finance and new lending protocols’, *Pressacademia*, Jan. 2023, doi: 10.17261/pressacademia.2023.1686.

[67] V. Koibichuk and T. Dotsenko, ‘Content and Meaning of Financial Cyber Security: a Bibliometric Analys is’, *Financial Markets Institutions and Risks*.

[68] G. Wang and M. Nixon, ‘SoK: Tokenization on blockchain’, in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2021. doi: 10.1145/3492323.3495577.

[69] E. R. Krishnan, ‘Understanding Decentralized Finance (DeFi) and how it’s changing the Global Financial Landscape’, in *Advances in Business Informatics empowered by AI & Intelligent Systems*, CSMFL Publications, 2023, pp. 20–33. doi: 10.46679/978819573220302.

[70] A. L. Johnson, ‘Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation’, Mar. 2016. [Online]. Available: http://scholarship.law.unc.edu/ncbi/vol20/iss1/15

[71] B. Liu, P. Szalachowski, and J. Zhou, ‘A First Look into DeFi Oracles’, May 2020, [Online]. Available: http://arxiv.org/abs/2005.04377

[72] B. Liu, P. Szalachowski, and J. Zhou, ‘A First Look into DeFi Oracles’, May 2020, [Online]. Available: http://arxiv.org/abs/2005.04377

[73] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, ‘SoK: Decentralized Finance (DeFi)’, Association for Computing Machinery (ACM), Sep. 2022, pp. 30–46. doi: 10.1145/3558535.3559780.

[74] J. Srinivas, A. K. Das, and N. Kumar, ‘Government regulations in cyber security: Framework, standards and recommendations’, *Future Generation Computer Systems*, vol. 92, pp. 178–188, Mar. 2019, doi: 10.1016/j.future.2018.09.063.

[75] A. N. Didenko, ‘Cybersecurity regulation in the financial sector: Prospects of legal harmonization in the European Union and beyond’, *Uniform Law Review*, vol. 25, no. 1, pp. 125–167, Mar. 2020, doi: 10.1093/ulr/unaa006.

[76] M. Peihani, ‘Regulation of Cyber Risk in the Banking System: A Canadian Case Study’, *Journal of Financial Regulation*, vol. 8, no. 2, pp. 139–161, Sep. 2022, doi: 10.1093/jfr/fjac006.

[77] K. Shah, D. Lathiya, N. Lukhi, K. Parmar, and H. Sanghvi, ‘A systematic review of decentralized finance protocols’, *International Journal of Intelligent Networks*, 2023.

[78] S. Vasudevan, ‘DeFi: A risky business or silver bullet for SMEs?’, in *International Conference on Cyber Resilience, ICCR 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICCR56254.2022.9995866.

[79] W. Li, J. Bu, X. Li, H. Peng, Y. Niu, and Y. Zhang, ‘A survey of DeFi security: Challenges and opportunities’, *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 10378–10404, 2022.

[80] ‘Decentralised Finance (DeFi) Risks: How to Protect Your Investments and Navigate the Crypto Landscape Safely - Alpha Development’. Accessed: Aug. 13, 2024. [Online]. Available: https://alphadevelopment.com/insights/decentralised-finance-defi-risks-how-to-protect-your-investments-and-navigate-the-crypto-landscape-safely/

[81] ‘The Limits of DeFi for Financial Inclusion | OECD’. Accessed: Aug. 13, 2024. [Online]. Available: https://www.oecd.org/en/publications/the-limits-of-defi-for-financial-inclusion_f00a0c7f-en.html

[82] ‘Top-5 cryptocurrency heists in history (so far) | Kaspersky official blog’. Accessed: Aug. 15, 2024. [Online]. Available: https://www.kaspersky.co.uk/blog/top-5-cryptocurrency-heists/25131/

[83] ‘The 5 largest cryptocurrency crimes in history | Crime + Investigation UK’. Accessed: Aug. 15, 2024. [Online]. Available:

https://www.crimeandinvestigation.co.uk/articles/4-largest-cryptocurrency-crimes-history

[84] 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.

[85] 'Rising Cyber Threats Pose Serious Concerns for Financial Stability'. Accessed: Aug. 19, 2024. [Online]. Available: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[86] 'White House attributes Ukraine DDoS incidents to Russia's GRU | CyberScoop'. Accessed: Aug. 13, 2024. [Online]. Available: https://cyberscoop.com/ukraine-ddos-russia-attribution-white-house-neuberger/

[87] S. AlBenJasim, T. Dargahi, H. Takruri, and R. Al-Zaidi, 'FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study', 2023, *Taylor and Francis Ltd.* doi: 10.1080/08874417.2023.2251455.

[88] M. Camillo, 'Cybersecurity: Risks and management of risks for global banks and financial institutions', *Journal of risk management in financial institutions*, vol. 10, no. (2), pp. 196–200, 2017.

[89] G. W. Peters, A. Chapelle, and E. Panayi, 'Opening discussion on banking sector risk exposures and vulnerabilities from Virtual currencies: An Operational Risk perspective', Dec. 01, 2016, *Palgrave Macmillan Ltd.* doi: 10.1057/jbr.2015.10.

[90] M. Alonso *et al.*, 'DeFi risks and the decentralisation illusion', 2021.

[91] N. Carter and L. Jeng, 'DeFi protocol risks: The paradox of DeFi', *Regtech, suptech and beyond: innovation and technology in financial services" riskbooks–forthcoming Q*, vol. 3, 2021.

[92] P. Winter, A. H. Lorimer, P. Snyder, and B. Livshits, 'Security, Privacy, and Decentralization in Web3', Sep. 2021, [Online]. Available: http://arxiv.org/abs/2109.06836

[93] I. Makarov and A. Schoar, 'Cryptocurrencies and decentralized finance (DeFi)', *Brookings Pap Econ Act*, vol. 2022, no. 1, pp. 141–215, 2022.

[94] G. Bello and A. J. Perez, 'Adapting financial technology standards to blockchain platforms', in *ACMSE 2019 - Proceedings of the 2019 ACM Southeast Conference*, Association for Computing Machinery, Inc, Apr. 2019, pp. 109–116. doi: 10.1145/3299815.3314434.

[95] C. Wronka, ‘Financial crime in the decentralized finance ecosystem: new challenges for compliance’, *J Financ Crime*, vol. 30, no. 1, pp. 97–113, Jan. 2023, doi: 10.1108/JFC-09-2021-0218.

[96] C. C. Okoye, E. E. Nwankwo, F. O. Usman, N. Z. Mhlongo, O. Odeyemi, and C. U. Ike, ‘Securing financial data storage: A review of cybersecurity challenges and solutions’, *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 1968–1983, doi: 10.30574/ijsra.2024.11.1.0267.

[97] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, ‘Cybersecurity threats in FinTech: A systematic review’, May 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.eswa.2023.122697.

[98] S. Ahmad, S. Wasim, S. Irfan, S. Gogoi, A. Srivastava, and Z. Farheen, ‘Qualitative v/s. Quantitative Research- A Summarized Review’, *Journal of Evidence Based Medicine and Healthcare*, vol. 6, no. 43, pp. 2828–2832, Oct. 2019, doi: 10.18410/jebmh/2019/587.

[99] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner, and B. Schlosser, ‘DeFining DeFi: Challenges Pathway’, in *2021 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2021*, Institute of Electrical and Electronics Engineers Inc., Sep. 2021, pp. 181–184. doi: 10.1109/BRAINS52497.2021.9569795.

[100] ‘Global cybersecurity workforce grows, but still confronts shortfall of 4M people | Cybersecurity Dive’. Accessed: Aug. 08, 2024. [Online]. Available: https://www.cybersecuritydive.com/news/cybersecurity-workforce-shortfall-4-million/698307/

[101] N. S. Uzougbo, C. G. Ikegwu, and A. O. Adewusi, ‘Regulatory frameworks for decentralized finance (DEFI): challenges and opportunities’, *GSC Advanced Research and Reviews*, vol. 19, no. 2, pp. 116–129, 2024.

[102] ‘Updated PCI DSS v4.0 Timeline’. Accessed: Aug. 22, 2024. [Online]. Available: https://blog.pcisecuritystandards.org/updated-pci-dss-v4.0-timeline

[103] ‘United Kingdom Country Guide | Elliptic’. Accessed: Aug. 23, 2024. [Online]. Available: https://www.elliptic.co/country-guides/united-kingdom

[104] ‘Country Guide for India | Elliptic’. Accessed: Aug. 23, 2024. [Online]. Available: https://www.elliptic.co/country-guides/india

[105] ‘Nigeria Country Guide | Elliptic’. Accessed: Aug. 23, 2024. [Online]. Available: https://www.elliptic.co/country-guides/nigeria

[106] ‘United States Country Guide | Elliptic’. Accessed: Aug. 23, 2024. [Online]. Available: https://www.elliptic.co/country-guides/united-states

[107] ‘China Country Guide | Elliptic’. Accessed: Aug. 23, 2024. [Online]. Available: https://www.elliptic.co/country-guides/china

[108] L. D. Oyeniyi, C. E. Ugochukwu, and N. Z. Mhlongo, ‘DEVELOPING CYBERSECURITY FRAMEWORKS FOR FINANCIAL INSTITUTIONS: A COMP REHENSIVE REVIEW AND BEST PRACTICES’, *Computer Science & IT Research Journal*, vol. 5, no. 4, pp. 903–925, doi: 10.51594/csitrj.v5i4.1049.

[109] A. Dey, ‘Enhancing Cyber Security in the Banking Domain: Innovative Problem Resolution’, *Journal of Artificial Intelligence & Cloud Computing*, pp. 1–6, Sep. 2022, doi: 10.47363/JAICC/2022(1)243.