Development of Cybersecurity Framework for FinTech: Bahrain as a Case Study

Salah Khalifa AlBenJasim

@00575552

School of Science, Engineering & Environment

University of Salford

A Thesis Submitted to Partially Fulfil the Requirements for the Degree of Doctor of Philosophy, September 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude and appreciation to my esteemed supervisors, Professor Haifa Takruri and Dr Rabab AlZaidi; your guidance, insights, and continuous support throughout this research journey have been instrumental in shaping the outcome of this thesis.

Additionally, I would like to thank Dr Tooska Dragahi, my previous supervisor, for her mentorship during the initial stages of this research.

Lastly, I extend my gratitude to all the professional and expert participants who generously shared their knowledge and expertise during this research journey. Your contributions, whether through interviews, surveys, or discussions, have provided valuable insights and perspectives that have enriched the depth and breadth of this study.

DEDICATION

I dedicate this work:

To the respected memory of my late father, who inspire me even in his absence. His guidance and love have shaped the person I am today, and I am forever grateful for his influence.

To my mother, the pillar of strength in my life,

To my beloved wife, Sharifa, your unwavering love, understanding, and constant encouragement have been my anchor throughout this challenging journey.

To my sons, Dr Khalifa, Dr Nasser, and Eng. Faisal, your accomplishments and dedication to your own pursuits have inspired me to strive for excellence.

To all my sisters, brothers, and family members, your positive encouragement and support have been invaluable in my academic and personal endeavours.

LIST OF PUBLICATIONS

1. **Salah AlBenJasim**, Tooska Dargahi, Haifa Takruri & Rabab Al-Zaidi (2023): FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2023.2251455.

   https://doi.org/10.1080/08874417.2023.2251455

2. **Salah AlBenJasim**, Haifa Takruri, Rabab Al-Zaidi, and Tooska Dargahi (2023): Development of Cybersecurity Framework For FinTech Innovations: Bahrain as a Case Study, Computers & Security Journal. (Under Review – Dec 2023)

LIST OF ACRONYMS AND ABBREVIATIONS

General

AI	Artificial Intelligence
API	Application Programming Interface
ATM	Automated Teller Machine
CFFB	Cybersecurity Framework for FinTech in Bahrain
COBIT	Control Objectives for Information and Related Technology.
CSOC	Cybersecurity Operations Centre
CSP	Cloud Service Providers
FINTECH	Financial Technology
GCC	Gulf Cooperation Council
GDPR	General Data Protection Regulation
ICT	Information Communication Technology
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
IT	Information Technology
KYC	Know Your Customer
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
PRISMA	Systematic Reviews and Meta-Analysis
SLR	Systematic Literature Review
SWOT	Strengths, Weaknesses, Opportunities, and Threats

Entities in Bahrain

BFB	Bahrain FinTech Bay
BIBF	Bahrain Institute for Banking and Financial
CBB	Central Bank of Bahrain
iGA	Information & eGovernment Authority
MOC	Ministry of Commerce
NCSC	National Cyber Security Centre
PDPL	Personal Data Protection Law
TRA	Telecommunications Regulatory Agency

LIST OF SOFTWARES AND RESEARCH TOOLS

Product	**Version**	**Usage**	**Website**
MS Office	365	Word Processing, Analysis, Graphics	www.office.com
MS Teams	365	Online meetings	www.office.com
EndNote	20	References management	www.endnote.com
NVivo	12	Qualitative data analysis	www.lumivero.com
SPSS	29	Statistical analysis	www.ibm.com/spss

DECLARATION

I hereby certify that the thesis I am submitting is an intellectual work of my own, entirely original in form. All sources from which thoughts, references, and derived extracts have been appropriately acknowledged. The thesis has not been presented anywhere else for assessment.

Salah Khalifa AlBenJasim
12 September 2024

ABSTRACT

For decades, the Kingdom of Bahrain has embraced the changes brought by technology through its commitment to further increase dynamism, creativity, and innovation. With the support of its business-empowering regulations, Bahrain strives to establish an ideal, secure, and streamlined environment for Financial Technology (FinTech) innovations and become a regional FinTech hub.

The COVID-19 pandemic increased the reliance on digital platforms as the world adapted to working remotely and performing online financial transactions. Cybercriminals seized the opportunity to exploit vulnerabilities in FinTech systems. Phishing attacks, ransomware, and data breaches have become more prevalent, targeting individuals and FinTech institutions. Bahrain, which is not different from the rest of the world, was impacted by such cyber threats. Thus, FinTech companies have had to strengthen their cybersecurity countermeasures and protocols to combat these threats.

Existing countermeasures in the literature primarily focus on general cybersecurity practices and frameworks, with limited attention given to the specific needs of the FinTech industry. Hence, the main research problem addressed in this study is the lack of a focused cybersecurity framework tailored to the specific needs of the FinTech industry in Bahrain. To bridge this gap, this research addresses the problem by conducting an extensive review of existing cybersecurity challenges, common practices, and cybersecurity standards and through in-depth research interviews with executives, experts, and other FinTech business stakeholders. Leveraging this knowledge, this research proposed a novel and adaptable framework that addresses the risks and vulnerabilities faced by FinTech innovations in Bahrain. The framework comprises six principles, the Capacity Building and Awareness, Regulation and Governance, Third Parties, Risk Management, Secure Service Delivery, and Best Practices. It involves twenty-four control activities, and fifty guidelines adopting a risk-based approach to address current and future technological advancements and potential threats.

The proposed framework was evaluated by industry experts through panel discussions and Delphi sessions, who confirmed its practical feasibility, ability to address specific risks, and compatibility with the existing FinTech regulatory landscape in Bahrain.

The adaptability and high acceptance of the proposed framework by industry experts highlight its novelty and potential to significantly enhance the cybersecurity resilience of the FinTech sector and establish Bahrain as a regional FinTech hub.

This page intentionally left blank

Chapter 1: Introduction

1. Chapter 1: Introduction

1.1. Research Background

Bahrain maintained an excellent reputation for its banking regulations and financial services systems. A total of 385 Banks and Financial Institutions operated in the country, with a qualified 14,148 workforce in the financial sector, as per the Central Bank of Bahrain (CBB) (W. CBB, 2019). Moreover, the financial sector plays a vital role in the socio-economic development of the Kingdom of Bahrain.

Bahrain has distinguished itself from its wealthier neighbours by the scale of its domestic market and the level of international competitiveness when it comes to being a technology centre, thus calling for regional cooperation. The aim is to be an entry point for international investors to the market sector and a provider of talent and innovation for Gulf Cooperation Council (GCC) countries.

The kingdom has a strategic plan in keeping with the regional trend, which points out how its economy should diversify from oil. Vision 2030 was introduced in 2008 and relies on the construction of state-of-the-art infrastructures to encourage private investment and promote entrepreneurship in sectors such as banking and financial services, real estate, tourism, logistics, and Information and Communication Technologies (ICT) (BFB, 2018).

Table 1.1 summarises the guiding principles of Vision 2030.

Table 1.1 The guiding principles of the Economic Vision 2030.

Sustainability	• The private sector should be able to drive economic growth in Bahrain independently. • Bahrain's Vision sees the economic prosperity built on a firm foundation. • Government finances will adhere to the principle of sustainability, upholding a system that is stable and forward-looking. • Bahrain will use its resources to invest in the future, improving its human capital through education and training, particularly in the field of applied sciences. • Economic growth must never come at the expense of the environment and the long-term well-being of Bahrainis. • No effort will be spared to protect Bahrain's environment and preserve the kingdom's cultural heritage.
Competitiveness	• Bahrain will attain a high level of competitiveness in a global economy. • Increased productivity comes about much more naturally in a competitive environment, driving economic growth, profitability, and wages.

	• Higher productivity requires people with the right skills for each position. • Bahrain will go to great lengths to educate its people, retain qualified staff, and attract foreign workers with the skills that are lacking. • The key is to make Bahrain a great place to do business for both local and foreign companies. • Many factors combined to make a country attractive to investors in high-value-added industries: a high-quality public service, a cutting-edge infrastructure, and an appealing living environment are among.
Fairness	• Bahrain's Vision is that the country's future economic success will impact society more widely, creating a broad base of prosperity. Every individual can make a worthwhile contribution to society, given the means and presented with the opportunity. • For fairness to be nurtured, all transactions made by both the public and private sectors must be transparent. • Free and fair competition should prevail, with private and public activities taking place in the open, whether they concern employment, land for public auction or the outcome of a tender. • The role of Bahrain is to provide the legal and regulatory framework that ensures the protection of consumers and fair treatment for business owners. • Stamping out corruption and seeing that laws are justly enforced. All are treated equally under the law, in accordance with international human rights, and everyone has equal access to services, namely education and health care, and that the needy are supported via adequate job training and a targeted social safety net.

By achieving this, Bahrain aims to establish itself as a centre for technology, innovation, and expertise, potentially impacting the region of the GCC nations to enhance their economic cooperation.

In the past five years, Bahrain has agreed to invest in FinTech's emerging trend to raise investment and economic growth. As a new acronym, FinTech has become a common term for the technology embraced by financial services institutions. FinTech innovation is technically enabled and can contribute to new business models, applications, services, and products that have an associated contextual influence on financial markets and services provision. FinTech developments are also fundamentally changing the way people access financial services. Simultaneously, the FinTech industry has become a prime target for cybercriminals due to the vast amounts of sensitive financial data they interact with. Due to the disintermediation of regulated firms or activities, some of these innovations could threaten the FinTech industry's financial stability.

This is the preliminary chapter of this research, and it will present the research aspects, beginning with the research background and factors that impact Bahrain's FinTech businesses.

The researcher's extensive experience in the field of cybersecurity, along with the local market review, helped find the main research problem and gaps that support the research focus area, leading to further investigation and the development of a well-structured framework to address these issues. The research problem is presented in this chapter, accompanied by research objectives and relevant research questions.

1.2. FinTech Innovation

Nowadays, financial services have become more reliant on information technology, where clients benefit from innovative delivery channels. It has witnessed a significant advancement in the banking systems to the extent that providing online banking services, exchanging, storing, and executing electronic transactions has become a fundamental means of work at all financial institutes mainly driven by customer needs. Financial Technology (**FinTech**) is disrupting the existing financial institution operations, making consumers aware that money transfer, investment, insurance, funding, financial inclusion, and other financial services will be entirely changed in a few years (Koffi, 2016).

Over the last five years, Bahrain has made a commitment to participate in the developing trend of FinTech in order to stimulate investment and foster economic development. FinTech innovation is facilitated by technology and leads to the development of novel business models, applications, services, or products that have a significant impact on financial markets and the supply of financial services. It provided a variety of advantages, in particular, improvements in performance and cost savings (Fadhul & Hamdan, 2020). FinTech developments are also fundamentally changing the way people access financial services. At the same time, some of these innovations could also potentially pose threats to financial stability due to the disintermediation of regulated firms or activities.

Despite FinTech's advantages in efficiency improvement for financial services channels, competition enhancement, and financial inclusion promotion, it creates new challenges that endanger financial institutes' stability and integrity in general. Cyber-attacks such as (Phishing, Denial of Service, Malware, etc.), are used to threaten the security of FinTech. Therefore, FinTech and its cyber-security regulations critically require researchers and practitioners to be adequately aware and up to date.

The financial sector's cybersecurity concerns, both in Bahrain and abroad, are increasing, and several cybersecurity issues have become rampant in recent times. The same Information

Communication Technology (ICT) that facilitates innovation is also being used by criminals to carry out cyber-attacks and other malicious cyber activities. Cyber-attacks and malicious cyber activities in the financial sector can lead to substantial financial losses for customers and banks. Other than creating trust deficits, it affects the institution's reputation and negatively impacts the economy. Financial Institutions are conscious of such potential threats and have taken several measures to protect themselves and their customers. Financial regulators worldwide mandate several security-related measures on financial institutions (A. Didenko, 2020). As such, banks and other financial institutions have improved their focus on cybersecurity by paying more attention to tackling the issues.

1.3. Emerging Attention of Cybersecurity in Bahrain

On the government side, the National Cyber Security Centre (NCSC), a national agency facilitating IT policies and related legislation among government entities, designed a new model which defines guidelines to assist government entities in the kingdom in enhancing information security by adopting a unified, systematic approach. The iGA has a dedicated directorate looking after the proper implementation of the mentioned model (iGA, 2019).

On the other hand, the Central Bank of Bahrain (CBB) is responsible for maintaining monetary and financial stability in the kingdom. The CBB, in its capacity as the regulatory and supervisory authority for all financial institutions in Bahrain, issues regulatory requirements that licensees and other specified parties are legally obliged to comply with. These regulatory requirements are contained in the CBB Rulebook (CBB, 2019). The Rulebook is divided into seven volumes (Figure 1.1), covering different areas of financial services activity. The CBB Law provides for two formal rulemaking instruments: Regulations and Directives, which have general application throughout the Kingdom and bind all persons ordinarily affected by Bahraini legislative measures. The CBB Rulebook is categorized either as Rules or as Guidance. Rules have a binding effect; if a licensee breaches a rule, it is liable to enforcement action by the CBB and, in some instances, criminal proceedings by the Office of the Public Prosecution. Guidance, on the other hand, leads the CBB to assess that the rule(s) to which the Guidance relates has been complied with, while failure to comply with Guidance is generally viewed as tending to suggest a breach of a Rule (CBB, 2019).

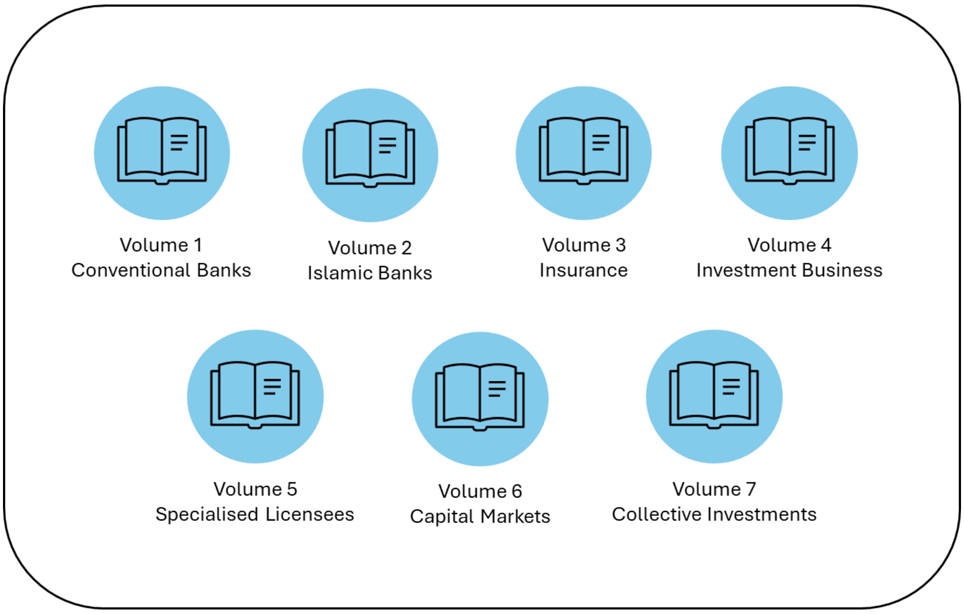


Figure 1.1 CBB RuleBook Volumes.

The sections of the CBB Rulebook relevant to cybersecurity contain requirements for conventional bank licensees operating in Bahrain to establish parameters and control procedures to monitor and mitigate cyber operational risks. These cybersecurity operation management controls, as summarised in Table 1.2, were circulated for all banks to safeguard their infrastructure and systems individually, which leads to different mitigation approaches and various structured actions.

Table 1.2 CBB's Cybersecurity controls (CBB, 2019).

Task	General Control	Purpose
Identify	Develop a bank-wide understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	The activities in the Identify Function are foundational for effective use of the Cyber Security Risk Management Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables a bank to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
Protect	Develop and implement appropriate safeguards to ensure the delivery of critical services.	The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity incident.

Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity incident.	The Detect Function enables the timely discovery of cybersecurity events.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain resilience plans and restore any capabilities or services that were impaired due to a cybersecurity incident.	The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident.

1.4. Research Problem

Due to its dependence on information technology for its online services and electronic transactions, in combination with connections for remote operation, FinTech has become increasingly vulnerable to cyber threats. A cyber-attack could, therefore, lead to monetary fraud and failure of information consistency and integrity, breach of the personal privacy protection that these institutes are committed to maintaining, and many more complications (Mehrban et al., 2020).

The financial technology (FinTech) industry is a prime target for cybercriminals due to the vast amounts of sensitive financial data they store. As a result, FinTech firms have been increasingly targeted by significant cybersecurity incidents in recent years. In 2021, a global report (Cassidy McCants, 2023) of financial institutions found that hackers increasingly preferred account takeovers as a method of attack. The report showed that the number of attempted takeovers had risen by 282% between 2019 and 2020.

In 2022, there were a total of 1,234 data breaches in the financial services industry. This represents a 10% increase from the previous year (Petrosyan, 2023).

Moreover, the average data breach cost in the financial services industry in 2023 is $5.9 million. This is significantly higher than the average cost of a data breach across all industries, which is $3.86 million (IBM_Security, 2023).

While users have become more competent, attackers have also become more sophisticated. In fact, 36% of data breaches are attributed to phishing attacks (Barahona, 2022). Recent phishing attacks include hackers impersonating banks to trick individuals into changing passwords or disclosing financial information over the telephone. Phishing emails pose a significant security threat to FinTech apps and users because of their ability to simulate authentic email messages closely.

According to Trend Micro, a combined 56,873,271 e-mails, URLs, malware, and banking malware attacks were recorded in the Gulf Cooperation Council (GCC) region during the first half of 2020 (Khaleej-Times, 2020). The multinational cybersecurity software company reported 41,236,550 e-mail threats, 13,181,016 URL victims, and 61,314 URL-hosted attacks. Malware detections in the GCC area continue to rise, with Trend Micro logging 2,392,097 malware detections and an additional 2,294 banking malware incidences.

In the first half of 2020, COVID-19-related threats were the most common type of risk encountered by organisations worldwide. Trend Micro blocked 8.8 million COVID-19-related attacks in six months, almost 92% of which were spam sent through e-mail. Trend Micro blocked 163,774 Covid-19 threats in the GCC, including 127,415 URL attacks, 36,312 e-mail spam attacks, and 47 malware attacks (Khaleej-Times, 2020).

Cybersecurity regulations for FinTech tend to contain generic, high-level guidelines that lack precision. Mainly when it comes to technology standards, cyber risks, threat types, or security compliance. Moreover, FinTech entities, mainly start-ups, have adopted a rapid development cycle for their services before launching them to the market – which requires a more robust balance between growth speed and cybersecurity resilience (A. Didenko, 2020).

While many cybersecurity studies were undertaken worldwide in the context of financial services, few types of research in the same field were conducted in Bahrain. This research will enable the regulator to bridge the gap between academic research and financial industry practice. To build the theoretical framework for the study, this research relies on the few empirical studies that have focused on Bahrain in the field of cybersecurity and FinTech.

Benefiting from worldwide contributions, some studies seek to analyse current cybersecurity risk management standards, namely ISO 27001 (Barlette & Fomin, 2010). However, these research studies mostly detail the benefits and drawbacks of these standards and how to apply and manage them. Some articles discuss cybersecurity frameworks such as the National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), and ISO 17799 as tools for regulatory fulfilment (Schlarman, 2007). In

(Sipior & Ward, 2008), the authors present a framework for cybersecurity management that considers global, national, corporate, and personnel factors.

This research analyses current international frameworks used in cyber risk management globally and the challenges FinTech has already faced. The innovative addition of this work is developing an adequate framework to handle cyber risk for FinTech in Bahrain.

1.5. The Motivation for the Research

The urgent need for this research in cybersecurity within Bahrain’s FinTech sector arises from several critical factors. Firstly, the escalating threats posed by cybercriminals employ sophisticated techniques such as social engineering, malware, and zero-day exploits to bypass existing defences. The allure of substantial financial rewards and the relatively low risk of apprehension make FinTech prime targets for these attacks.

Secondly, with the rise of cloud computing, mobile banking, and interconnected systems, the evolving landscape of technology trends introduces new attack vectors and expands the potential impact of breaches. This necessitates a comprehensive evaluation of vulnerabilities and risks associated with these technology advancements to develop effective cybersecurity strategies to protect FinTech systems.

Thirdly, the protection of sensitive personal and financial data held by FinTech is of paramount importance. Data breaches not only erode consumer confidence but also trigger regulatory sanctions. Robust data protection mechanisms are essential to prevent unauthorised access and breaches, ensuring the security and privacy of sensitive information.

Fourthly, cyberattacks targeting the FinTech sector transcend national borders, emphasising the need for collective action and knowledge sharing across the industry. The global nature of the FinTech system requires collaboration and information exchange to combat cyber threats effectively. Research can contribute to a collective understanding of the international scope of cyberattacks, enabling the development of coordinated strategies to protect Bahrain’s FinTech systems.

Finally, while existing research addresses specific aspects of cybersecurity, there is a critical gap in comprehensively assessing the overall posture and readiness of FinTech institutions. A comprehensive understanding of vulnerabilities, strengths, and weaknesses is necessary to address emerging challenges effectively. Bridging this gap through research will generate valuable insights and recommendations to develop the cybersecurity framework for FinTech, safeguard sensitive information, maintain consumer trust, and mitigate risks associated with cyber threats.

1.6. Research Gap

Although cybersecurity in the FinTech industry has gained considerable attention in recent years, there is a noticeable lack of research on developing a tailored cybersecurity framework, particularly for FinTech stakeholders. This research seeks to bridge this gap by analysing the unique cybersecurity challenges and conditions experienced by the FinTech businesses in Bahrain.

Current research on cybersecurity frameworks for the FinTech industry often adopts a broad approach and neglects to account for country's unique characteristics. Although there have been studies on cybersecurity concerns in the broader Middle East area and worldwide, there is a shortage of research explicitly focusing on Bahrain's FinTech industry. This study addresses the existing knowledge gap by presenting a comprehensive understanding of the cybersecurity concerns and threats FinTech stakeholders encounter specifically in Bahrain.

Furthermore, several existing cybersecurity standards are primarily designed for conventional financial institutions or general technological settings. Nevertheless, the unique characteristics of FinTech, such as the use of cutting-edge technology, cloud computing, open Application Programming Interfaces (APIs), and decentralised systems, need a customised approach to promoting cybersecurity. Presently, a limited amount of research focuses on developing a cybersecurity framework tailored explicitly for the FinTech sector in Bahrain. This research aims to provide a valuable contribution by proposing a framework that aligns with the particular FinTech requirements, cyber risks, and regulatory guidelines of the FinTech stakeholders in Bahrain.

Additionally, the cybersecurity ecosystem is constantly evolving, frequently emerging newer threats and attack vectors. Keeping up with the latest cybersecurity best practices and tactics in the FinTech sector is challenging due to the quick pace of technical advancements and the dynamic nature of the FinTech industry. The current body of research studies may not sufficiently address the increasing risks and weaknesses that are distinct to the FinTech ecosystem in Bahrain. This study will focus on combining the most up-to-date knowledge into the cybersecurity framework to ensure it remains applicable and effective in minimising the impact of evolving cyber threats.

Lastly, while several studies have concentrated on developing cybersecurity frameworks, there is often insufficient attention given to assessing the efficiency of these frameworks and consistently enhancing them over time. It is essential to evaluate the effectiveness of the suggested framework, identify any deficiencies or constraints, and provide suggestions for improvements. This work aims to fill this gap by including an evaluation factor to measure the efficiency of the proposed cybersecurity design and provide methods for ongoing improvement.

This study aims to fill the existing research gaps in the field of cybersecurity in the FinTech industry, with a particular focus on Bahrain. By doing so, it will enhance the current body of knowledge on this subject. The results will not only be advantageous to the local players in Bahrain but also provide significant insights and suggestions for other countries and areas that have comparable FinTech ecosystems.

1.7. Research Main Question and Objectives

FinTech, in general, requires a robust cybersecurity framework to control both their business and technical operations. Thus, to investigate the critical aspects involved in developing such a framework for FinTech in Bahrain, this study will answer the below research question:

What are the crucial elements in developing a Cybersecurity Framework designed for FinTech entities in Bahrain?

The research aims to develop a cybersecurity framework, along with common cybersecurity controls, to support FinTech by protecting them from cyber risks. A framework that ensures efficiency by creating a balance that optimises its advantages while lowering potential cyber threats to the financial system. Therefore, a well-defined cybersecurity guideline (framework) will contribute significantly to achieving this target.

The research question is extended into the following research objectives and more focused research questions.

Specifically, within the context of cybersecurity, the objectives of this research are:

1. To review significant risks facing FinTech innovations within Bahrain’s financial sector and security monitoring tools used for interpreting malicious activities.

2. To determine what governance elements are in place addressing FinTech systems protection.
3. Data collection by interviewing experts to investigate the incident response plans, vulnerability management, and prevention actions in case of any compromised system, and to evaluate end user’s behaviours and skills in the context of cybersecurity, and what education, training, and awareness reinforcement are needed.
4. Analysing the collected data to develop a cybersecurity framework for FinTech in Bahrain. A framework that can be shared seeking for assuring cybersecurity in all FinTech entities consistently yet appreciates the differences in business environments.
5. To validate the proposed cybersecurity framework and test its applicability.

The above objectives were investigated and achieved via getting answers to the research sub-questions that will be discussed in Chapter 3.

1.8. Significance of the Study

As technology advances, the possibility of cyber-attacks, security breaches, and fraud becomes a common concern. As a result, cybersecurity is critical to the success and evolution of FinTech. Similarly, regulation and governance policies must be dynamically synchronised with such advancement. Although their guidebooks have been updated concerning cyber-threat precautions, the CBB has not adequately addressed specific guidelines for FinTech operational systems. Therefore, these regulations and controls must be updated to cater to FinTech and cyber threats when integrating with financial systems (Fadhul & Hamdan, 2020).

Additionally, cyber-attacks on banking, FinTech, and financial infrastructures can significantly impact individuals, corporations, and even the country's economy. Various security risk assessment, attack detection, and security monitoring approaches must be reviewed and identified to improve protection and resilience. The existing methods, however, are not entirely governed by any specific cybersecurity policies, procedures, or standards on a unified manner. Threat alerts, plans for incident response, vulnerability management, and prevention actions in case of any compromised system are managed by each institute individually. In general, the communication between banks in the context of cybersecurity is poorly handled, and relevant incident information is not shared, creating space for malicious activities to pass undetected to other banks’ infrastructure. Furthermore, capacity building for end-users, who form the weakest link in the context of cybersecurity, needs to be levelled up across the financial sector.

1.9. Research Impact

The research is expected to have a significant impact on multiple stakeholders and domains. The primary impact of this research will be on the FinTech stakeholders in Bahrain, including financial institutions, technology providers, and individual users. The cybersecurity framework developed through this research will provide practical guidance and recommendations for these stakeholders to enhance their cybersecurity practices. By implementing the framework, FinTech innovations can strengthen their resilience against cyber threats, protect their customers' data and financial transactions, and safeguard their reputations. This, in turn, will contribute to maintaining customer trust and confidence in the FinTech ecosystem, leading to sustained growth and innovation in the sector.

Moreover, the research findings and recommendations will have an impact on policymakers and regulators in Bahrain. The insights provided by the research will assist in shaping cybersecurity policies and regulations specific to the FinTech sector. CBB can leverage the research outcomes to establish a robust regulatory framework that addresses the unique cybersecurity challenges faced by FinTech stakeholders in Bahrain. The research impact may result in developing cybersecurity controls, guidelines, and compliance requirements, ensuring a secure and regulated environment for FinTech operations.

Along with the above, enhancing the FinTech sector's cybersecurity has broader national security implications. Bahrain, being a regional hub for FinTech, recognises the importance of protecting critical financial infrastructure and systems from cyber threats that can potentially disrupt the economy and compromise national security. The research impact will strengthen the overall cybersecurity posture of Bahrain's financial ecosystem, reducing the risk of cyber incidents that could have a cascading effect on the country's economy and stability.

Additionally, the research impact extends beyond the national level, as the findings and recommendations can be relevant and applicable to other countries and regions with similar FinTech ecosystems. The research outcomes may foster international collaboration and knowledge-sharing among policymakers, regulators, and cybersecurity experts. This collaboration can lead to developing best practice guidelines, cross-border cybersecurity initiatives, and harmonising cybersecurity standards in the global FinTech community.

1.10. Scope of the Study

The primary purpose of this study is to contribute to the existing body of knowledge and comprehension of the contextual factors influencing cybersecurity controls, with a specific focus on FinTech innovation in Bahrain. It conducts a comprehensive review of the cybersecurity literature for FinTech in Bahrain and abroad. In general, this research looks into the definition of FinTech, highlights the cyber challenges that FinTech faces, and discusses the existing measures that can effectively manage FinTech cybersecurity risks. Considering Bahrain as a case study, this research provides an overview of the commonly adopted cybersecurity guidelines issued by CBB and the cybersecurity standards in the FinTech industry worldwide. The research findings were obtained via the analysis of the interview data that were gathered between January 14th and March 5th, 2023. This research included interviews with a sample of 14 FinTech executives, IT professionals, bankers, and cybersecurity experts with extensive competency in the banking industry and years of experience in the IT and cybersecurity field. These individuals were selected to represent various financial sector entities in Bahrain. Considering Bahrain's FinTech regulation is in its early stages, the proposed framework should ensure an optimum option by creating a balance that optimises its advantages while lowering potential cyber threats to the financial system. Bahrain is used as a research field to illustrate the critical aspects involved in developing such a framework through a research method that will be explained in chapter 3.

1.11. Research Contributions

We observed that various existing frameworks and standards have several strengths and drawbacks that encourage or restrict their adoption. How does the proposed framework differ from existing frameworks and standards? What contributions will this work add to academia, industry, and society? We attempt to address these questions in this section.

To effectively develop an appropriate framework, this research assessed existing frameworks and analysed key factors relevant to Bahrain's FinTech regulations. If these factors aren't identified, and requirements aren't analysed, adopting a common standard just because it's widely used may be acceptable in some instances but excessive or insufficient in others. In this situation, there is no one-size-fits-all solution, and investing in implementing a certain standard should be carefully evaluated (Brotby, 2009). No research supports a particular standard as a solution for all cybersecurity risks for financial institutes. This is where a customised approach may be the most appropriate answer. A tailored framework takes personnel expertise and turns it into a streamlined model that incorporates regulatory standards. Instead of utilising the standards' proposed contents, this study will find an inventory of threats, vulnerabilities, and risks unique to the FinTech businesses in Bahrain. Associated controls and control objectives must also be tailored to the risky nature of the FinTech companies (US_GAO, 1999). A locally customised framework can develop and evolve while remaining closely aligned with FinTech's risk management.

Following the identification of the threats, vulnerabilities, and risks relevant to FinTech and the analysis of existing standards, fundamental aspects and principles should be included to develop a cybersecurity framework for FinTech firms.

This is a pioneering study that explores different aspects to provide the basis for developing a competitive cybersecurity framework for FinTech. It is hoped that this study will have a substantial contribution on the research and practice areas by offering the following:

1.11.1. Contribution to Academia:

While this research contributes to academic research and bridges a gap in cybersecurity for FinTech, the researcher participated in writing research papers and articles that focus on the cybersecurity for financial deployment approach. Using the outcomes of this study lays the foundation for future studies to measure the effectiveness of such a framework when deployed in FinTech firms. Moreover, future researchers can extend such a model to other critical infrastructures, such as government and other industry-specific systems.

1.11.2. Contribution to Industry:

From a practitioner's perspective, the research leads to a novel financial-specific framework that can be shared among all local financial entities, ensuring better cybersecurity. The proposed framework is expected to be a competitive alternative to complex models and standards that need added resources. Additionally, it endeavours to raise the level of cybersecurity through governance, operational processes, human capacity building, and technology elements. This will result in a continuously trusted electronic environment for FinTech and financial services in Bahrain and a sign for regional and global leadership.

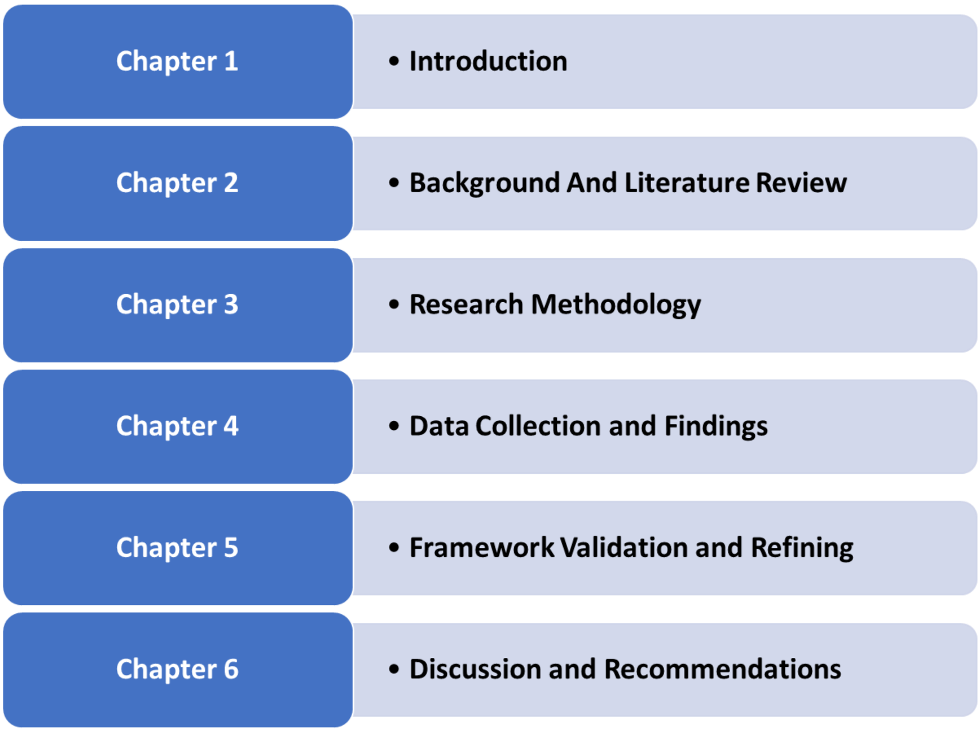
Furthermore, the study will generate business opportunities for local consultancy agents with international cybersecurity partners to establish a FinTech excellence centre for cybersecurity aiming to strengthen Bahrain's financial infrastructure and provide cybersecurity services to local banks and FinTech institutes. Cooperation with CCB supervising the centre for regulation and compliance will further increase the opportunities.

1.11.3. Contribution to the Society:

Raising the level of cybersecurity awareness is key to protecting and safeguarding public users from any cyber threats and risks. In this direction, the researcher published a short article in the same context in a local newspaper. Moreover, participation in other public events themed around cybersecurity and financial services will be planned to positively impact the level of cybersecurity awareness in society.

1.12. Thesis Structure and Outline

The following is a brief of this thesis's structure and outline, as shown in Figure 1.2:



Chapter 1	• Introduction
Chapter 2	• Background And Literature Review
Chapter 3	• Research Methodology
Chapter 4	• Data Collection and Findings
Chapter 5	• Framework Validation and Refining
Chapter 6	• Discussion and Recommendations

Figure 1.2 Thesis Structure and Outline

Chapter 1 introduces the research topic and the cyber threats FinTech businesses face worldwide and in Bahrain. It establishes the context for the study and how fintech innovation emerged. It presents precise, measurable objectives based on the study's gap analysis and research question. The significance of the study, research impact and contributions are also discussed. It concludes by summarising the key points discussed and setting the stage for the subsequent thesis chapters.

Chapter 2 provides a comprehensive background and literature review of the research topic. It includes three parts based on the Systematic Literature Review (SLR) approach: FinTech, cybersecurity, and the relationship between FinTech and cybersecurity. The first part explores the status of FinTech and its corresponding challenges from current research and relevant past studies. The second part is dedicated to cybersecurity, including definitions, risks, countermeasures, and different types of cyber threats in the FinTech ecosystem. The consecutive sections in this part are for cybersecurity controls, human factors, initiatives, and common standards and frameworks. Additionally, some obstacles to implementing cybersecurity standards and frameworks are also included. The final part of this chapter reveals the overlap area between cybersecurity and FinTech and articulates the importance of cybersecurity governance to FinTech innovations in the Kingdom of Bahrain. A careful examination of past study contributions leads to the research gap that underpins this research.

Chapter 3 outlines the research methodology employed in the study. The research philosophy, research approach, techniques, and design are discussed. The chapter also addresses the research instrument, analytic technique, rationale, and pilot survey on Bahrain's FinTech firms. It includes sections such as data collection and analysis, results validation, ethics considerations, and research limitations. The chapter concludes by justifying the chosen methodology and addressing the study's potential limitations.

Chapter 4 describes the data collection process and presents the findings obtained from the collected data. The description of the sample, general characteristics of the participants, data collection method, and participants' privacy and confidentiality are all presented in this chapter. It identifies FinTech stakeholders in Bahrain and presents thematic results through a qualitative data analysis approach. The chapter concludes by summarising the key findings and detailed proposed framework's controls.

Chapter 5 focuses on validating and refining the proposed cybersecurity framework for FinTech. It includes framework validation using the Delphi approach and expert review. The chapter concludes by discussing the implications that resolve the intended research question.
Chapter 6 comprehensively discusses the research findings and provides recommendations based on the results. It includes the evaluation of the research question, fulfilment of research objectives, contributions of the study, and study limitations. It concludes with some suggestions for research extensions and future research directions.

Finally, the thesis includes a list of references and appendices. The References part includes a comprehensive list of all the sources cited throughout the study. It encompasses scholarly articles, books, reports, conference papers, and other relevant sources that have contributed to the research and supported the arguments and findings presented in the thesis. At the same time, the appendices' part includes additional materials that supplement the main body of the research. These materials are included to provide further details and supporting evidence that may not be suitable for inclusion within the main thesis's text.

1.13. Summary

In this chapter, concerns about cybersecurity in financial institutes and FinTech, particularly, were recognised based on a short analysis of the literature and the researcher's professional background in the field. The research is based on the fact that Bahrain's financial systems have become a target for numerous cyber-attacks in the region, besides an increased number of individuals performing their regular banking activities over a wide range of financial electronic channels. A short discussion of the research background, FinTech innovation, and emerging attention of cybersecurity in Bahrain are the first parts of this chapter. The research gap and research problem were established for further investigation. Next, the research problem, research gap, research main question, and objectives are highlighted. The significance of the study, the research impact and contributions, the explanation of the research limitations, and the thesis's outline are all presented in this chapter.

The following chapter comprehensively reviews the literature concerning FinTech innovations and the cybersecurity landscape, including technologies, countermeasures, solutions, and several cybersecurity frameworks, in addition to benchmarking techniques aiming for the development of a cybersecurity framework. This may be accomplished by investigating key factors to develop a framework for FinTech in Bahrain. The research endeavours to raise the level of cybersecurity and a trusted electronic environment for both the customers and FinTech in Bahrain.

Chapter 2: Background and Literature Review

2. Chapter 2: Background And Literature Review

2.1. Introduction

The advent of the Automated Teller Machine (ATM) was the most significant financial revolution in banking history. Previously, telegraphs were used to conduct financial transactions, which had been the case since 1838. The banking sector utilised information technology to achieve this goal and optimise its procedures (Eyal, 2017). The rise of the Internet in the globe brought in a wave of technological innovations in various fields. FinTech is a relatively new concept and innovative financial business that uses technology to enhance financial transactions (Schueffel, 2016). FinTech is a new term referring to current interactions, particularly Internet-related technology (such as cloud computing and mobile Internet), financial services, and operational processes (for example, transferring money and banking transactions). FinTech represents a disturbance to the financial industry due to automated processes and ICT availability. FinTech offers a range of business models in the financial services industry that integrate security, speed, and innovation (Casoria, 2018).

Based on the efforts of some international organisations and global standard-setting entities, a modern conceptual model is developed to illustrate the paradigm, as shown in Figure 2.1, called the “FinTech Tree” (Ehrentraud et al., 2020).

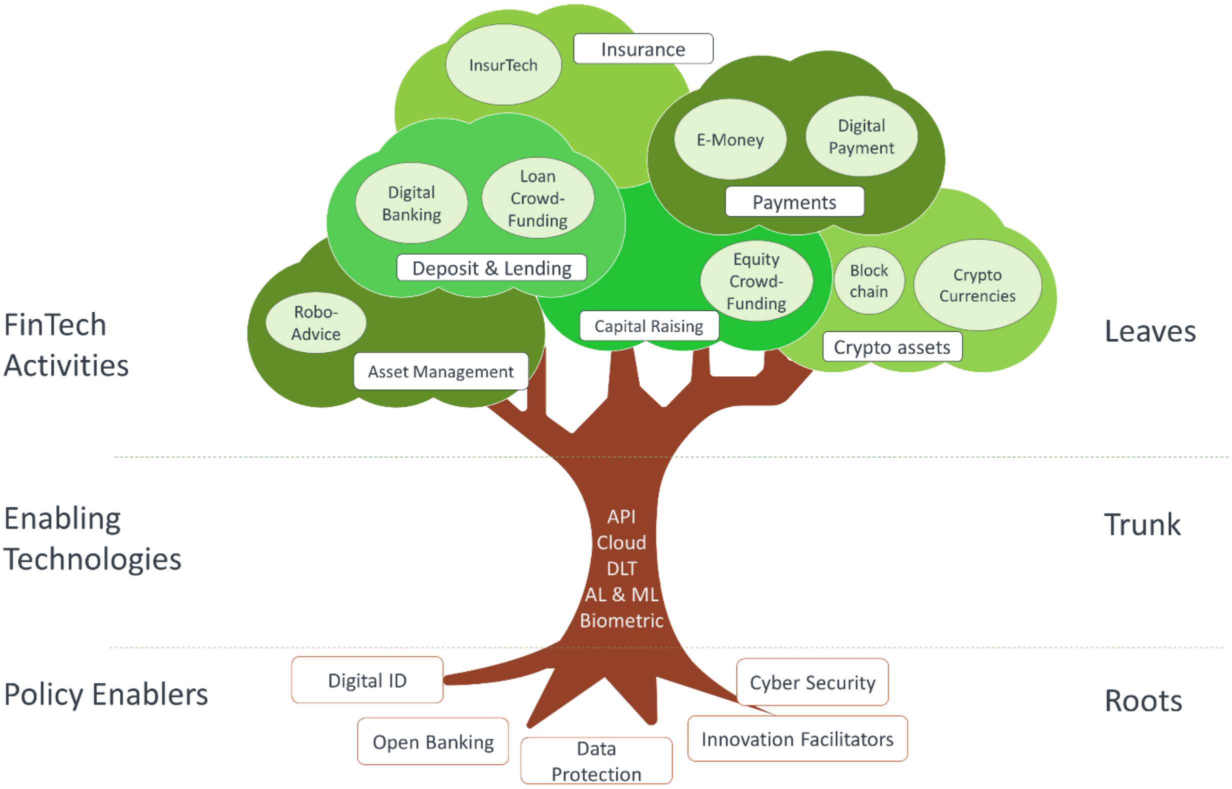


Figure 2.1 FinTech tree: a taxonomy of the FinTech environment. (Ehrentraud et al., 2020)

FinTech tree differentiates between three categories, namely, FinTech activities, enabling technologies, and policy enablers. These activities are performed in various financial sectors and take different forms.

After the global financial crisis in 2008, advances in e-finance and mobile technologies for financial organisations fuelled FinTech innovation. This evolution was characterised by integration in financial system innovation, Internet technology, networking services, social media, artificial intelligence, cloud computing, and big data analytics.

As the digital society widens, the actual risk of destructive cyber-attacks is constantly rising and puts pressure on all financial organisations to evolve and develop more viable cybersecurity protection measures (Davis et al., 2017). Within FinTech contexts, cybersecurity is critical in protecting businesses from losing their competitive edge. Indeed, today's vital financial systems are exposed to various cyber threats that may disrupt the whole business model. In today's fast-paced environment, cybersecurity is anticipated to become an intrinsic element of institutes' strategy, design, and operations that adopt the FinTech paradigm. Table 2.1 demonstrates the state of a data breach in Europe, the Middle East, and Africa (EMEA), as per the Data Breach Investigations Report 2021 (Bassett et al., 2021).

Table 2.1 The state of Data breach in EMEA

Frequency	5,379 incidents, 293 with confirmed data disclosure
Top Patterns	Basic Web Application Attacks, System Intrusion and Social Engineering patterns represent 83% of breaches.
Threat Actors	External (83%), Internal (18%) (breaches)
Actor Motives	Financial (89%), Espionage (8%), Fun (1%), Grudge (1%) (breaches)
Data Compromised	Credentials (70%), Internal (52%), Personal (22%), Other (16%) (breaches)

According to Trend Micro, 56,873,271 e-mails, URLs, malware, and banking malware attacks were recorded in the Gulf Cooperation Council (GCC) region during the first half of 2020 (Khaleej-Times, 2020). The multinational cybersecurity software company reported 41,236,550 e-mail threats, 13,181,016 URL victims, and 61,314 URL-hosted attacks. Malware detections in the GCC area continue to rise, with Trend Micro logging 2,392,097 malware detections and an additional 2,294 banking malware incidents.

This chapter presents a Systematic Literature Review (SLR) of FinTech cybersecurity concerns and existing risk management strategies. It helps to identify similarities across globally recognised cybersecurity standards and frameworks. Bahrain is used as a case study to explore key characteristics and factors not fully addressed while adopting such standards. The results can assist Bahrain's financial regulators in understanding these issues. It establishes the groundwork for a FinTech cybersecurity framework for Bahrain and aspires to improve cybersecurity and trust in the electronic environment for clients and service providers.

2.2. Prior Research

There have been relatively few SLRs done on the topic of FinTech and Cybersecurity. (Zavolokina et al., 2016) highlighted that FinTech was more than just the use of information technology in finance. According to certain literature, FinTech may be viewed as start-ups, services, technologies, firms, digitalisation, industry, new generations, opportunities, products, and risks. (Mehrban et al., 2020) provide a comprehensive survey of FinTech by reviewing the most recent and anticipated privacy and security issues in the financial industry. The research paper comprehensively analyses current security issues, detection mechanisms, and security solutions proposed for FinTech. Numerous cybersecurity threats exist within the realm of

FinTech, and research has highlighted how these weaknesses can lead to financial setbacks, damage to reputation and legal liability for FinTech firms (Barbu et al., 2021; Kaur, Habibi Lashkari, Habibi Lashkari, et al., 2021; Najaf et al., 2020). Furthermore, researchers have examined the different cybersecurity measures FinTech companies might implement to shield themselves and their clients against cyber-attacks (Barbu et al., 2021; Kaur, Habibi Lashkari, Habibi Lashkari, et al., 2021; Najaf et al., 2020).

In the same domain, (Taylor et al., 2020) shed light on future directions of research, education, and practices in the blockchain and cybersecurity space. Moreover, there has been continued interest in investigating the potential of Artificial Intelligence (AI) to improve the vulnerability assessment of FinTech systems (McKinnel et al., 2019). Vučinić et al. developed a FinTech Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis matrix to review its strengths, weaknesses, opportunities, and threats. It continues by outlining the modern management idea of "Risk-based thinking" as a strategy for dealing with the challenges and opportunities that FinTech may present. The research examines cyber risk in the FinTech sector as the most recent and significant concern emerging from these chaotic and unpredictable times (Vučinić & Luburić, 2022).

Despite the wide range of literature on cybersecurity in FinTech, a few studies have identified research gaps and limitations. Some studies, for instance, have focused on certain types of cybersecurity threats or countermeasures. In contrast, others focused on only the perspectives of FinTech businesses, ignoring the attitudes of consumers and regulators (Barbu et al., 2021). Other studies have also addressed the regulatory frameworks for FinTech cybersecurity. Nevertheless, some researchers have noted that these frameworks may not be adequate to address all FinTech industry cybersecurity concerns (Najaf et al., 2020).

Conducting a literature review is essential to improve the understanding of academics, industry actors, and regulators about the FinTech sector's protection from cyber threats. As a result, a comprehensive synthesis of previous research efforts, particularly in the domains of FinTech and cybersecurity, is essential, as presented, to lead future research activity.

2.3. Systematic Literature Review (SLR)

Literature reviews are helpful sources for knowledge generation by systematically assembling existing scientific work and using direct or thematic analysis of explicit or tacit information synthesis to address particular research questions (Schryen et al., 2015). This work follows

Schryen et al. published method for the SLR, resulting in an approach suitable for research in various sectors where there may be variations in what is considered relevant.

The SLR is a technique for selecting and analysing scientific papers to offer evidence for identifying published research for FinTech and cybersecurity that is complete, explicit, and reputable. The SLR process used is shown in Figure 2.2 using the (PRISMA) set layout, which stands for Preferred Reporting Items for Systematic Reviews and Meta-Analyses (Moher et al., 2010).

The PRISMA guidelines, published in 2009, aim to assist systematic reviewers in providing clear and comprehensive reporting of the purpose, methods, and findings of their literature reviews (Moher et al., 2010). In the last years, improvements in the methodology and terminology used in systematic reviews have made it necessary to update these guidelines. The PRISMA 2020 statement (Page et al., 2021) supersedes the 2009 version and incorporates updated reporting guidelines that encompass the latest developments in techniques for identifying, selecting, evaluating, and synthesising research studies. The structure and presentation of the items have been altered to enhance the ease of implementation as shown in Figure 2.3.

The resulting PRISMA structure considers an initial batch of papers, known as the baseline sample, which was found using keywords in scientific search engines. This sample is completed by applying exclusion and inclusion criteria to create an intermediate sample. Then, using reverse searches to include publications not found in the first searches limits the final sample for analysis, referred to as the synthesis sample. Finally, the synthesis sample is subjected to a descriptive analysis before being reviewed through a thematic analysis to address the research questions.

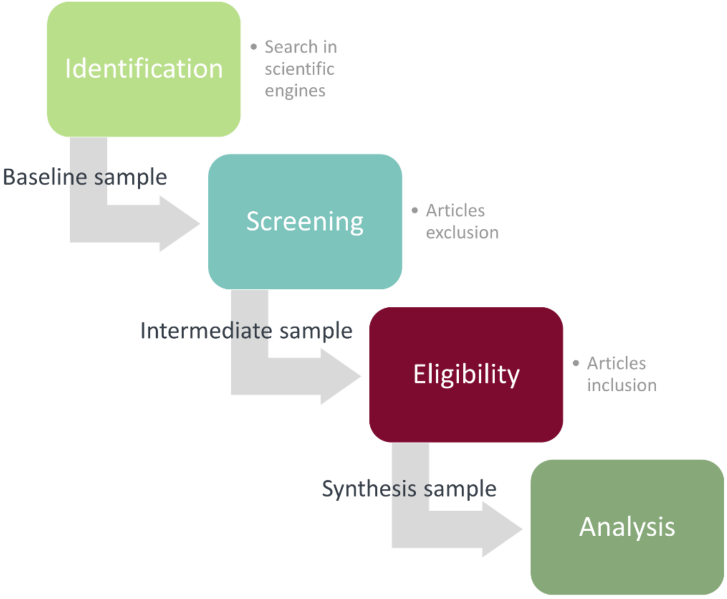


Figure 2.2 PRISMA set layout for the Systematic Literature Review (Moher et al., 2010).

2.4. Materials and methods

2.4.1. Initial search

The purpose of SLR is to show the findings of employing a replicable technique to collect and synthesise information on the existing cybersecurity frameworks and FinTech proposed by the scientific community to identify the research gap in the context of the Kingdom of Bahrain.

This phase included formulating the approach to carry out the search in the databases. A preliminary assessment was conducted to investigate the topic of study and see if there were any published articles on the subject, as well as any studies addressing the specific requirements that may form the foundation for the proposed research questions in the review by providing answers to the following three questions:

1. How to define FinTech and cybersecurity concepts and, what are the cyber challenges facing FinTech companies?
2. What are some of the cybersecurity countermeasures, guidelines, standards, and frameworks that are relevant to the FinTech industry?
3. Why is there a need to develop a cybersecurity framework specifically for FinTech entities in Bahrain?

Answers to these questions give information to assist comprehension of the current research on topics related to cybersecurity and FinTech, encourage cross-pollination among research methodologies, and provide suggestions for prospective cybersecurity frameworks for FinTech in Bahrain.

2.4.2. Systematic Search

In this SLR, we use the sources of scientific databases listed in Table 2.2 to analyse diverse data sources. All of them are highly indexed databases, and provide extensive indexing coverage, enabling a larger number of results from various sources and journals of varying levels.

Table 2.2 Sources of scientific databases

Scientific Databases	**URL**
Google Scholar	(scholar.google.com)
ScienceDirect	(www.sciencedirect.com)
Scopus	(www.scopus.com)
Web of Science	(www.webofknowledge.com)

The SLR was conducted from June 2021 until November 2022, after which we analysed the results.

In order to maintain a consistent approach to the search process, we identified the keywords related to the subject of interest that required to be analysed. Additionally, we bought their synonyms from a thesaurus. The keywords include Cybersecurity, cyber security, cyber threats, Financial Technology, FinTech, and Bahrain. The formulation of the search equation using logical operators that combined these keywords aimed to provide more precise search results of the titles, keywords, and summaries in the database. Table 2.3 lists all search formulation queries that were used to identify the first batch of papers:

Table 2.3 Search Queries

Database	**Search Queries using Keywords**
Scopus	(“Cybersecurity” OR “cyber security”) AND (“FinTech”) OR “Bahrain”
Web of Science	(“Cyberattack*” OR “cyber threat*” AND (“security”) AND “FinTech”) OR “Bahrain”
Google Scholar	(“Cybersecurity” OR “cyber security”) AND (“Banking” OR “Financial Technology” OR “FinTech”) OR “Bahrain”
ScienceDirect	"Bahrain" OR "Cybersecurity" AND "FinTech"

After the search was completed, the articles undergo screening based on the criteria for inclusion and exclusion. This often entails checking if papers' titles and abstracts satisfy the requirements.

2.4.3. Inclusion and exclusion criteria

The definition of inclusion and exclusion criteria for the SLR shown in Table 2.4 is essential for ensuring the quality of research processes. Inclusion criteria are the particular features of the sample being studied that are relevant to the purpose of the study. Exclusion criteria, on the other hand, are features of the sample that, even if they satisfy the inclusion criteria, are thought to introduce biases or quality shortcomings that could hinder the success of the research (Page et al., 2021).

Table 2.4 Criteria for the inclusion and exclusion of articles in the SLR.

	Criterion
Inclusion	1. The article is indexed in a credited scientific database. 2. The article simultaneously cites the phrases "FinTech", “cybersecurity”, and "Bahrain" in the title, abstract or keywords. 3. Studies were published between 2016 and 2022. 4. Studies published in English.
Exclusion	1. Article text not wholly written in English. 2. Studies qualify as either an article, editorial or review. 3. The article is older than 2016. 4. Studies fail to meet the relevance focus on the research topic. 5. Studies that target industries other than the financial and banking sectors.

2.4.4. Data Management

A total of 153 publications centred around the subject were initially identified. Nevertheless, to ensure a current perspective, publications from 2016 and 2022 were selected, with some older but important articles and references included. This has reduced the publications to 126. It was further filtered using the language, i.e., English language, and the scope, i.e., cybersecurity within the financial industry context. This has further reduced the publications to 92 related to the topic and matches the screening criteria.

Furthermore, EndNote software was used to assess the publications chosen and track the authors' comments on each one. EndNote keeps useful records, such as the paper's title, authors, publication year, reference, abstract, and keywords.

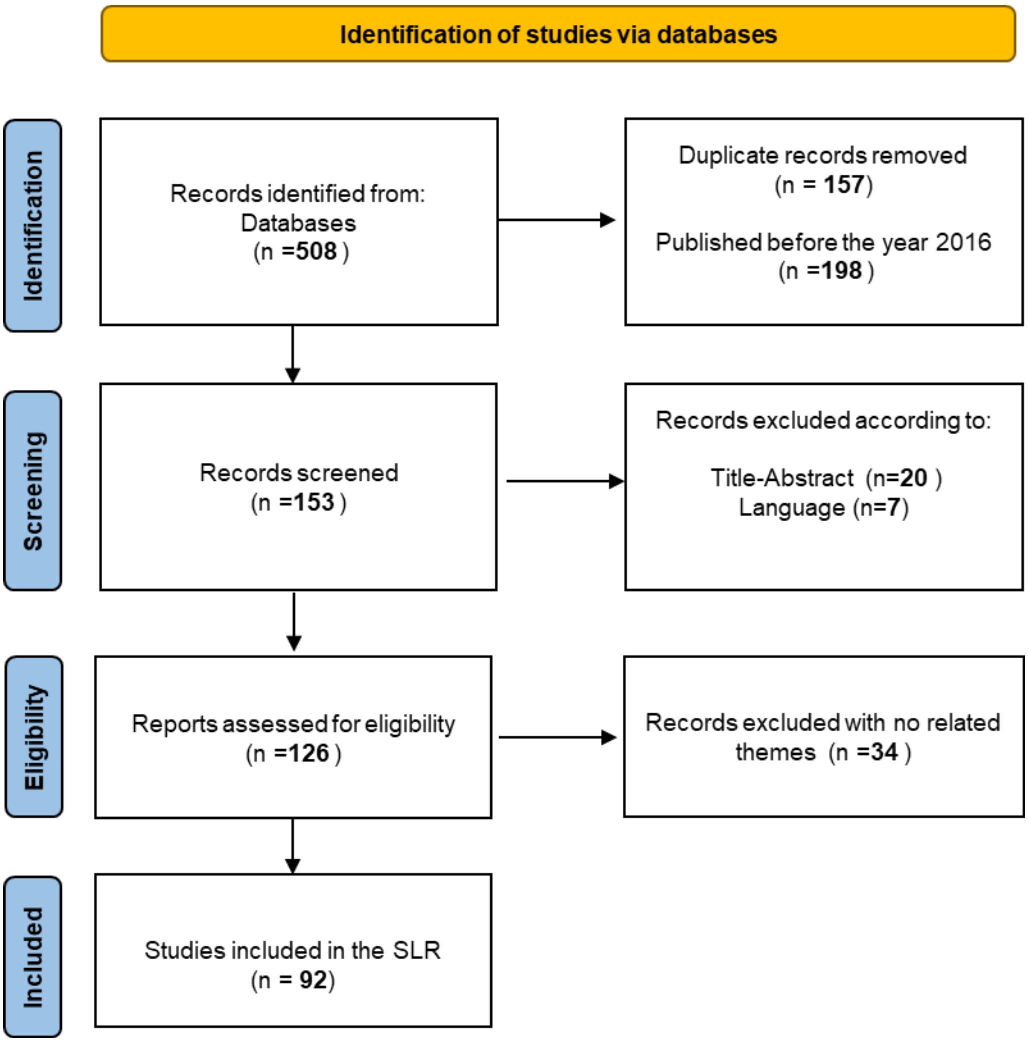

Identification of studies via databases
Identification
Records identified from: Databases (n =508)
Duplicate records removed (n = 157)
Published before the year 2016 (n =198)
Screening
Records screened (n =153)
Records excluded according to:
Title-Abstract (n=20)
Language (n=7)
Eligibility
Reports assessed for eligibility (n =126)
Records excluded with no related themes (n =34)
Included
Studies included in the SLR (n = 92)

Figure 2.3 Flow chart of the SLR selection process using PRISMA 2020 (Page et al., 2021).

2.4.5. Selection Process

The next step of the paper evaluation included a rigorous examination of the most important contents identified for each article. The key findings were addressed after the same categories of information were compared across all the publications. The following areas were explicitly considered:

1. A review of the FinTech and cybersecurity concepts and definitions.
2. Description of cybersecurity in terms of cyber risks, system security vulnerabilities, cyber threats, cyber-attacks, and remedies to be taken.
3. Cybersecurity regulations, guidelines, controls, and frameworks for FinTech.
4. Bahrain’s FinTech innovations and its cybersecurity initiatives.
5. Few book chapters were considered.

2.5. Results and Thematic Analysis

In this section, the findings of the thematic analysis are explained. We present the word cloud of all areas scanned in the literature search and the general topics categorisation applied in this research. Furthermore, cybersecurity challenges, issues in FinTech, and existing international cybersecurity frameworks and standards were compared. Finally, we shed light on Bahrain’s FinTech cybersecurity considerations.

2.5.1. Descriptive Analysis of Search Results

NVivo is a software specifically designed to facilitate the qualitative research approach. More precisely, it is employed for the analysis of unstructured text, auditory, visual, and pictorial information, including various sources such as interviews, focus groups, surveys, and journal articles (Leech & Onwuegbuzie, 2011).

The word count in terms of '% weight' (Table 2.5), which represents the number of characters as a proportion of the overall source, was generated using NVivo's constant comparison analysis tool.

Table 2.5 Word Count of % weight

Word	Length	Count	Weighted Percentage (%)
FinTech	7	177	1.54
financial	9	166	1.45
cybersecurity	13	111	0.97
security	8	106	0.92
technology	10	95	0.83
cyber	5	78	0.68
information	11	68	0.59
framework	9	54	0.47
services	8	53	0.46
systems	7	42	0.37
cloud	5	33	0.29
digital	7	32	0.28
organisations	13	32	0.28
Bahrain	7	30	0.26

Word clouds are useful for visually representing word count, as shown in Figure 2.4. They are easy to use and give fast insights at a look-through depiction of word frequency. The bigger the word appears in the graphic created, the more often the keyword occurs in the analysed text.

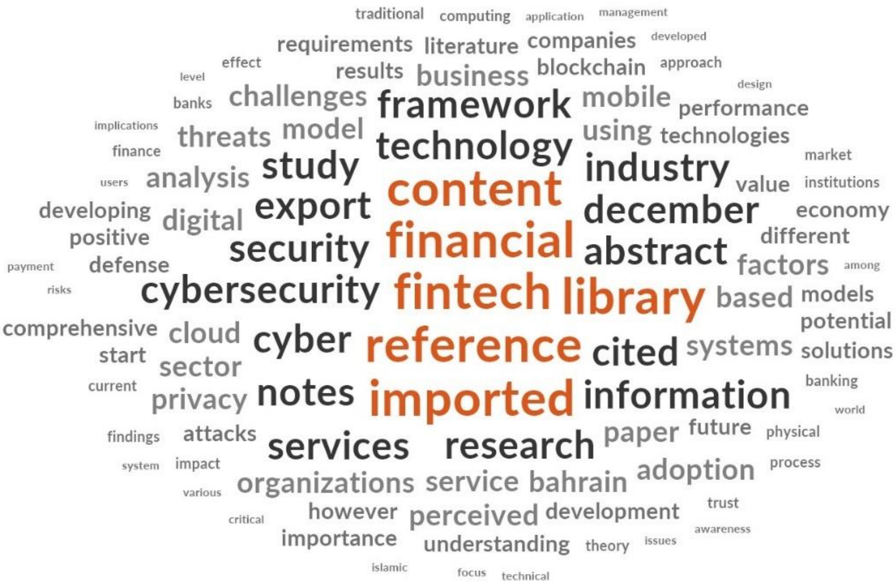


Figure 2.4 Word Cloud for keywords.

2.5.2. Thematic analysis

A thematic analysis is carried out to dig further into FinTech-related issues. NVIVO software is used for selective coding, customising it to the study questions requirements. As a manner of addressing the research objectives of this study, the thematic analysis categorises the articles in the synthesis sample according to the characteristics of the frameworks these articles discuss and/or apply. The categorisations that are applied in this SLR are presented in Table 2.6:

Table 2.6 Thematic Analysis Categorization

Definitions	FinTech
	Cybersecurity
Cyber Threats	Risks
	Threats
	Countermeasures
Managing Cybersecurity Risks	Guidelines
	Cybersecurity Frameworks
FinTech in Bahrain	FinTech Initiatives
	Banking regulations

There are a variety of viewpoints and definitions for cybersecurity and FinTech in the literature. Table 2.7 provides a set of FinTech definitions.

Table 2.7 A set of FinTech Definitions

FinTech Definitions	Reference
FinTech, a mixture of finance and technology, may have been around for a while. One of this term's first uses goes back to the 1980s	(Group, 2018)
FinTech is an industry composed of companies that use technology to make financial systems and the delivery of financial services more efficient.	(Ancri, 2016)
Technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.	((ECB), 2017)
A cross-disciplinary subject that combines Finance, Technology Management and Innovation Management.	(Leong & Sung, 2018)
Any innovative ideas that improve financial service processes by proposing technology solutions according to different business situations, while the ideas could also lead to new business models or even new businesses.	(Leong & Sung, 2018)

Technologically-enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.	(Gray & Leibrock, 2017)

The common context that repeats in several cybersecurity definitions as provided in Table 2.8 was considered from some research papers:

Table 2.8 Cybersecurity definitions.

Cybersecurity Definitions	**Reference**
The ability to protect or defend the use of cyberspace from cyber-attacks.	(NIST Kissel, 2011)
Preservation of confidentiality, integrity, and availability of information in the cyberspace.	(Standardization, 2005)
All activities necessary to protect cyberspace, its users and impacted persons from cyber threats.	(ENISA, 2017)
The protection of information assets by addressing threats to information processed, stored, and transported by the Internet-worked information systems.	(ISACA, 2016)
Prevention of damage to, protection of, and restoration of computers electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	(CNSSI, 2015)

2.6. Cybersecurity Challenges and Issues in FinTech

In the FinTech businesses, cybersecurity is the top challenge and a primary legislative concern (Hakmeh, 2018). Cyber attacks threaten systemic financial stability and may deter FinTech adoption. As a result, preventative measures must be implemented immediately and extended throughout the product and service lifecycles. This requires robust and effective controls to prevent and mitigate severe issues in privacy, cybersecurity, denial of service attacks, insider threats, malware injection, insecure APIs, shared vulnerabilities, and data security (Magnuson, 2018). Table 2.9 lists the significant challenges and issues in FinTech.

Table 2.9 Challenges and Issues in FinTech

Challenges and Issues in FinTech	**Reference**
Risks in business operations	(Gai, Qiu, & Elnagdy, 2016),(Liao et al., 2011),(Nussbaumer et al., 2012),(Shim & Shin, 2016),(Gai, 2014),(Ni et al., 2013)
Threats in FinTech	(Gai, 2014),(Gai, Qiu, Sun, et al., 2016),(Wang et al., 2015) (Guo et al., 2011)

Regulatory requirements	(Overy, 2018), (Group, 2018; Magnuson, 2018)
Importance of experimental data	(Overy, 2018),(Mehrban et al., 2020)
Financial privacy protection	(Sánchez et al., 2012),(Li et al., 2015),(Li et al., 2019),(Elnagdy et al., 2016)

As the financial industry as a whole continues to embrace digitisation further, so does the difficulty of protecting consumer data from cyberattacks, which are facilitated by an ever-growing attack surface. Scheau et al. (Şcheau et al., 2022) argue that appropriate cybersecurity rules and regulations must be implemented from both technical and human standpoints to keep up with the rapid adoption of technological improvements in the financial services industry. Figure 2.5 demonstrates the following levels and how they are linked to the cyber threats for FinTech businesses:

- The organisational assets that hackers may use to access FinTech systems make up the attack surface. This surface, which comprises human, digital, and physical assets, may be substantial for many businesses.
- An attack vector, which might include ransomware, compromised credentials, phishing, and malware, is a technique used by hackers to enter the attack surface.
- The risks posed by cyber-attacks.
- Countermeasures to address cybersecurity matters.

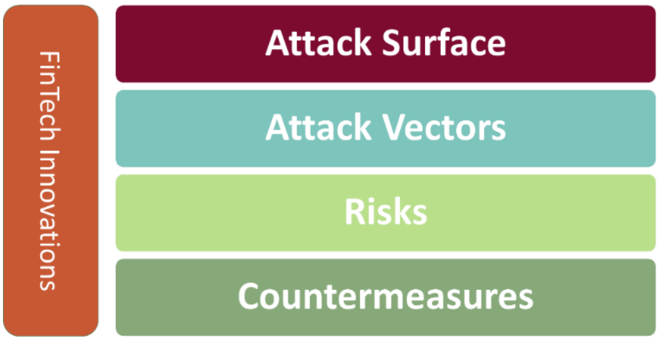


Figure 2.5 Cyber Threats for FinTech Businesses

FinTech businesses rely heavily on their information systems, so a well-structured framework would be essential to them. By following recognised information security standards, a well-established FinTech will most likely comply with regulations, often even before they become licensed. Therefore, part of the countermeasures is to have a cybersecurity framework or standard that protects systems and mitigates risks of cyber threats and vulnerabilities.

2.7. Cybersecurity Standards and Frameworks

Cybersecurity in FinTech is a relatively new technology focus, so there is no dedicated cybersecurity framework for the field. However, some general information security frameworks and standards exist that regulators request businesses follow to stay safe against cyberattacks. These frameworks could be considered for FinTech infrastructure. The governance bodies and related components in each cybersecurity standard or framework are presented in Table 2.10.

Table 2.10 Governance bodies and frameworks

Governance bodies and Frameworks	Description	Governance Type	Region	Components	Reference
NIST	The National Institute of Standards and Technology (NIST Kissel) is an NGO specialising in cybersecurity and publishing a cybersecurity framework that can be used in practically any sector.	Framework	USA	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Protective Technology • Anomalies and Events • Security Continuous Monitoring • Detection Processes • Response Planning • Communications • Analysis • Mitigation • Improvements • Recovery Planning	(Albastaki & Manta, 2020; Casoria, 2018; Hu et al., 2019; Huang, 2018; Magnuson, 2018)
PCI-DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a security standard that applies to all merchants and businesses that accept branded credit cards or other major credit card systems.	Standard	Global	• Builds and maintain a secure network, • Protect cardholder data, • Maintain a vulnerability management program, • Implement strong access control measures, • Regularly monitor and test networks, • Maintain an information security policy	(Smith, 2019; Syafrizal et al., 2020)
COBIT	COBIT (Control Objectives for Information and Related	Framework	Global	**Governance of Enterprise IT**	(Kabanda, 2018; Malatji et

	Technologies) is a framework created by the Information Systems Audit and Control Association (ISACA) for IT management and IT governance.			• Evaluate, Direct and Monitor (EDM) **Management of Enterprise IT** • Align, Plan and Organise (APO) • Build, Acquire and Implement (Al Duhaidahawi et al.) • Deliver, Service and Support (DSS) • Monitor, Evaluate and Assess (MEA)	al., 2019; Smith, 2019; Syafrizal et al., 2020)
ISO 27001	The ISO 27001, known as the information security management standard,	Standard	Global	• Information security policies. • Organisation of information security. • Human resource security. • Asset management. • Access control. • Cryptography. • Physical and environmental security. • Operations security. • Communications Security • System acquisition, development, and maintenance • Supplier relationships • Information security incident management • Information security aspects of business continuity management • Compliance	(Shen, 2014; Smith, 2019; Syafrizal et al., 2020; Wang et al., 2015)
GDPR	A privacy framework that specifies how organisations must secure their customers' or users' personally identifiable information	Regulation/ Framework	EU	• Breach Response, • Data Governance, • Risk Assessment, • Compliance Management	(Albastaki & Manta, 2020),(Syafrizal et al., 2020),(Canelón et al., 2019)

These standards and frameworks may be used as a reference, developed, modified, or integrated with other standards as required to address unique issues or audit for conformity with laws or regulations in place in a specific industry or nation (Syafrizal et al., 2020). Furthermore, an analysis is carried out to identify whether any comparable components exist across all standards and frameworks, as shown in Table 2.11.

Table 2.11 Analysis of cybersecurity standards and frameworks components

No	Name of Standards	Information Security Policies	Asset Management	Access Control	Incident Management	Risk Management	Risk Assessment	Security Assessment	Governance	Resilience	Personal Awareness and Training	Information Protection	Monitoring	Communication	Analysis	Recovery Planning	Monitoring Activity	Business Continuity Plan	Compliance
1	**ISO/IEC 27001**	✓	✓	✓														✓	✓
2	**COBIT 5**		✓			✓	✓		✓					✓			✓		
3	**NIST**	✓	✓	✓		✓	✓		✓		✓	✓		✓	✓	✓			
4	**GDPR**						✓		✓										✓
5	**PCI DSS**	✓		✓													✓		

Three to eleven similar components are owned by the selected five standards and frameworks based on an analysis of the many parts that belong to each standard and framework. There are a total of 18 parts that are common to those found in cybersecurity frameworks and standards.

Categories in the NIST cybersecurity framework that have been associated with ISO/IEC 27001, NIST, COBIT 5, etc., are just a few examples of the many cybersecurity standards and frameworks that have components that are mapped with other standards. Industry standard, such as PCI-DSS, is very detailed and strict; it includes many elements distinct from the general norm.

ISO implementations are widely recognised, particularly in the financial sector, due to regulatory compliance requirements. Although it is the simplest to automate and use for developing information security policies and performing automated information security risk assessments, many organisations that undertake ISO certifications concentrate on marketing benefits and neglect to recognise that being certified does not always imply that you are secure.

On the other side, because the NIST framework is very system-oriented and excludes organisational matters, there is an absence of a comprehensive view of cybersecurity risk management. NIST is primarily aimed at large organisations and may not apply to small businesses. In contrast to ISO 27001, NIST prescribes not only a risk assessment methodology but also at least some risk assessment. NIST, like ISO27000, offers a set of security measures and a guide for implementing the framework.

PCI DSS is regarded as an exceptional standard because its implementation is mandated by regulatory authorities and carefully monitored for effectiveness and potential flaws. However, implementing it properly would demonstrate a greater understanding of security needs and strengthen enterprises' immunity to external and internal threats.

A GDPR standard is often an obligation that the responsible organisation or regulatory body expects the implementing entity to adhere to in line with any applicable laws or regulations. It concentrates mainly on these areas: breach response, data governance, risk assessment, and compliance management.

Like other standards, COBIT's complexity prevents some businesses from adopting it because they lack the personnel and resources to achieve this goal. For many small businesses and other organisations where IT is not mission-critical or needed for existence, ISACA published a light version of COBIT named "COBIT Quick Start" to address complex matters. This version of COBIT is referred to as a special form of COBIT and may be used as a baseline. Businesses may also use it as a foundation for their transition to a decent level of cybersecurity management and governance.

From Table 2.11, some areas like incident management, security assessment, resilience, and monitoring are not being addressed well in the analysed standards. At the same time, the NIST framework offers a higher coverage of all other components.

2.8. Examples of Successful Cybersecurity Frameworks for FinTech from Other Countries

Various effective cybersecurity frameworks have been implemented across the global financial sector. Some examples are from the United States, Europe, Asia, and the Middle East.

In the United States, the NIST Cybersecurity Framework is widely utilised across industries, including finance, offering guidance for private sector organisations to assess and enhance their ability to prevent, detect, and respond to cyber-attacks (Shen, 2014). Bank of America, for example, has aligned its information security controls and annual policy management cycle to the NIST (America, 2019). Similarly, the European Union's Directive on Security of Network and Information Systems (NIS Directive) enforces legal measures to elevate cybersecurity levels, requiring essential service operators in the banking sector to implement appropriate security measures and report significant incidents to national authorities. The NIS Directive has been implemented by the European Central Bank, resulting in the creation of a unified framework for cybersecurity across EU financial institutions ((ECB), 2017). Moreover, in Singapore, the Monetary Authority of Singapore (MAS) has published the Technology Risk Management Guidelines, outlining risk management principles and best practices for financial institutions (A. N. Didenko, 2020). Similarly, Japan's Cybersecurity Basic Act, enacted in 2015, establishes a comprehensive framework for critical infrastructure cybersecurity, including financial institutions, by safeguarding personal information, setting cybersecurity standards, and promoting international cooperation (Nomakuchi, 2018).

In the Middle East region, the Dubai Financial Services Authority (DFSA) in the United Arab Emirates (UAE) has introduced the Cyber Risk Framework, aligning with the NIST Cybersecurity Framework to assist financial institutions in identifying, assessing, and managing cybersecurity risks (Schilirò, 2021). Likewise, the Saudi Arabian Monetary Authority (SAMA) has developed a cybersecurity framework based on international standards like ISO/IEC 27001 and the NIST Cybersecurity Framework, encompassing guidelines for risk management, incident response, and regulatory compliance to enhance the security of the financial sector (Albastaki & Manta, 2020).

The more widespread FinTech innovations emerge, the more likely regulators will take notice to guarantee that the information systems underlying these innovations are adequately protected and controlled (Haddad & Hornuf, 2019; Mawgoud et al., 2019; Mulligan et al., 2019). In section 2.12 (Discussion and Analysis), we will further analyse the need to develop a cybersecurity framework for FinTech specifically for Bahrain.

2.9. Bahrain FinTech Security Considerations

Even though Bahrain is a regional leader in the use of FinTech applications, there is a shortage of research in this field. Table 2.12 depicts the research papers that address topics related to FinTech in Bahrain.

Table 2.12 Primary studies on FinTech focused on Bahrain as a case study.

Topic	**Key Theme and Outcome**	**Reference**
User motivation for adopting FinTech services in Bahrain	Technology Acceptance Model (TAM) applied to analyse user motivations for FinTech adoption in Bahrain.	(Abdulkarim, 2021)
Adoption of FinTech and the future of digital wallets in Bahrain	Examines adoption of digital wallets as a form of FinTech in Bahrain and its future potential.	(Ahmed et al., 2020)
Importance of cybersecurity systems in banking and finance	Highlights the critical role of cybersecurity systems in managing risks within the banking and financial sector.	(Al-Alawi & Al-Bassam, 2020)
Factors influencing cybersecurity awareness in banking	Investigates the factors that influence cybersecurity awareness among banking sector employees.	(Al-Alawi & Al-Bassam, 2021)
Critical cybersecurity threats faced by Bahraini organizations	Identifies and discusses major cybersecurity threats faced by organizations in Bahrain.	(Al-Alawi et al., 2020)
Cybersecurity incidents in cyber-physical systems: A review	Reviews cases of cybersecurity incidents within cyber-physical systems.	(Al-Mhiqani et al., 2018)
Entrepreneurship as a driver for Bahrain's economy	Explores the potential of entrepreneurship to revitalize Bahrain's economy.	(Al-Shakar, 2017)
Strategies for implementing FinTech in banking	Explores innovative strategies for integrating FinTech solutions within the banking sector.	(Albastaki & Manta, 2020)
User adoption and satisfaction with FinTech in Bahrain	Investigates user adoption and satisfaction levels regarding FinTech services in Bahrain.	(Ali et al., 2021)
Cybersecurity as an enterprise risk in Bahrain	Analyses cybersecurity as a risk factor within the Bahraini legal framework for businesses.	(Casoria, 2018)

Evaluating cybersecurity readiness and its impact on performance	Evaluates the cybersecurity preparedness of organizations and its influence on their performance (Focus not specific to Bahrain).	(Hasan et al., 2021)
FinTech and agility as the future of Islamic finance in Bahrain	Examines how agility and FinTech can shape the future of Islamic finance within Bahrain's banking system.	(Raza Rabbani et al., 2021)
The propensity of bankers in Bahrain to use FinTech	Analyses the factors influencing bankers' inclination towards using FinTech solutions in Bahrain.	(Razzaque et al., 2020)

While some GCC states seem to be technologically prepared to deal with cyber-attacks, having spent resources to address the increasing quantity and frequency of threats, regulatory obstacles exist despite the current sector-based rules and processes (Hakmeh, 2018). However, dealing with such difficulties on a local and international level would be one of the GCC's priorities in the future (Hakmeh, 2018). Meanwhile, businesses and financial institutions must be aware that, given the rapid evolution of technology, one of their primary areas of intervention must be the pre-assessment of potential threats, which, when combined with a risk-mitigation strategy, should help minimise the effect of cyber-attacks on business operations and contribute to the protection of data exchanged and safeguard consumers and professional operators participating in the FinTech ecosystem (Casoria, 2018).

(Casoria, 2018) analysed the current state of the legislation in Bahrain and the GCC, emphasising the need for a more comprehensive legislative framework, as well as investments in cutting-edge technology, to raise the level of security and, as a result, disrupt cyber-threats. (Ali et al., 2021) investigate and evaluate Bahraini consumers' usage of FinTech services and their satisfaction with them. All of the characteristics studied, including accessibility, ease of use, completeness, accuracy, security, reliability, responsiveness, service quality, system quality, and information quality, all had a substantial positive influence on user satisfaction.

According to the Bahrain FinTech Bay (BFB) Ecosystem report (BFB, 2022), Bahrain has a lot of potential for FinTech investments, as it currently has three blockchain-enabled financial services, one mobile wallet (BenefitPay: consumers can make or receive payments via the mobile platform), one Peer to Peer crowdfunding form, and the Central Bank of Bahrain CBB-built sandbox. Bahrain has a high degree of regulatory activity, according to reports (Al-Alawi et al., 2021).

According to Al-Mhiqani et al. (Al-Mhiqani et al. 2018), cyberwarfare, cybercrime, hacktivism, and cyber espionage are the cybersecurity risks that Bahraini FinTech is most exposed to, according to previous events. Furthermore, some of the key reasons for inadequate cybersecurity and growing financial cybercrime in Bahrain's financial sector are as follows (Al-Alawi et al., 2020).

Several Bahraini banks use outdated password-based authentication methods, which provide inadequate protection and authentication. This weakness enables criminals to effortlessly breach user accounts via credential stuffing and brute-force assaults. Furthermore, the dependence of financial institutions on outdated security techniques, such as perimeter-based defences, has proven useless in safeguarding against recent, highly sophisticated risks such as advanced persistent attacks and insider threats. Moreover, the lack of knowledge about encryption exposes sensitive information to the risk of being intercepted and accessed by cybercriminals (Al-Alawi & Al-Bassam, 2020).

Inadequately designed or verified backup and recovery plans at some banks have facilitated ransomware actors' seizing data and forced financial institutions to make substantial ransom payments to restore their operations. Many Bahraini banks do not have dedicated, specialised cybersecurity teams, which means that IT managers lack the essential ability to detect, mitigate, and react to sophisticated cyber-attacks.

(Al-Alawi & Al-Bassam, 2021) emphasised that the insufficient knowledge among IT professionals at local banks about the most up-to-date cybersecurity standards and optimal procedures has made the implementation of sufficient security measures difficult. Consequently, this has created vulnerabilities that cybercriminals may take advantage of. Furthermore, they highlighted that the delayed implementation of important updates and security patches has enabled attackers to exploit well-known vulnerabilities and illegally penetrate systems.

Empirical evidence depicts that financial risk has the primary contributing role among the four particular risk variables driving total perceived FinTech risk. After financial risks, Bahrain bankers emphasise that factors such as legal, security, and operational risks are among the difficulties their clients incur while engaging in FinTech transactions (Razzaque et al., 2020). Furthermore, the study highlights the issues that need to be addressed. Factors influencing human awareness, such as knowledge, attitude, and behaviour, were identified, and the Value-Focus-Thinking method was used to define cybersecurity focus areas. The six focus areas were collected, including dedication to cybersecurity policy, effective password use, safe Internet and email use, being aware of cyber risks, backing up essential data, and mandatory operating system and antivirus software upgrades (Al-Alawi et al., 2020). Al-Bassam (Al-Alawi et al., 2020) examined the variables affecting the adoption of cybersecurity awareness in Bahrain's financial industry and identified a gap between "top management commitment and support, budgeting, cybersecurity policy enforcement, cybersecurity compliance, and cybersecurity culture."

2.10. CBB’s Cybersecurity Controls for FinTech

The CBB has established the foundations of legislative and regulatory rulebooks that support the implementation of banks in the financial sector, including an articulation of measures to ensure stability and regulations to combat cybercrime-related risks. While the link between security risk and user perceptions of overall FinTech risk is significant, it has been at least partially compensated for by Bahrain bankers (Razzaque et al., 2020). They implemented countervailing technical measures, as they are aware of the threats to cybersecurity and privacy posed by the rise of FinTech.

The CBB’s rulebook contains regulations on electronic banking, electronic payments, and cybersecurity risk management, aligning itself with international organisations' principles, notably the Basel Committee on Banking Supervision (Razzaque et al., 2020). The part on risk management for electronic banking and electronic money activities essentially demonstrates that banks should identify, assess, manage, and control the risks related to electronic banking and money. Furthermore, the threats associated with digital banking should be identified and controlled prudently. Because of the substantial effect that such risks might have, the role of overseeing cyber risks has been placed on the board of directors and senior directors of financial institutions. In terms of cybersecurity risk management, CBB’s rulebook mandates that all financial institutions prepare for cyberattacks by adopting adequate response mechanisms that must be assessed on a regular basis to guarantee that licensed institutions are capable of dealing with cyberattacks. The CBB has some other initiatives that embrace the establishment of a Regulatory Sandbox that permits FinTech firms, licensees, and start-ups to provide innovative financial and banking solutions(Albastaki & Manta, 2020). Moreover, (Al-Alawi et al., 2020) stated that only 20% of organisations in Bahrain are prepared to withstand cyber-attacks and security.

2.11. The Socio-Technical Systems Theory

In this section, the existing literature that has employed theoretical frameworks to study complex organizational and technological systems is reviewed. It highlighted key concepts, models, and empirical findings and examined the complex interplay between technology, people, processes, and the environment in FinTech systems.

The Socio-Technical Systems theory (STS) is an approach designed to optimise the alignment and correlation of a system's social and technological aspects while taking into account the system's environment. FinTech firms are complex socio-technical systems that include not just software and hardware activities but also individuals, tangible assets, and stakeholders (Castro et al., 2020). As highlighted in Chapter 1, the primary goal of this study is to propose a cybersecurity framework to aid in the identification and proper response to any vulnerabilities that may arise in current cybersecurity measures for FinTech.

Although the basic STS theory has generally stayed unchanged throughout the years, particular applications and general principles have evolved to match the changing nature of technology and work patterns (Davis et al., 2014).

Socio-technical systems are characterised by a significant degree of social complexity and technological complications that are designed to accomplish crucial societal functions (Baxter & Sommerville, 2011). They represent the harmonious combination of people, technology, organisational structures, and processes, including the operational context in which all of these elements take place (Carayon et al., 2015). According to (Whitworth, 2009), a socio-technical system is not composed of two distinct and adjacent systems but rather a fully integrated system. The interaction between social and technological systems involves the performance of tasks by teams and individual team members, as well as the complex interconnections of the system development life cycle (Troyer, 2016). (Bostrom & Heinen, 1977) and (Walker et al., 2007) provide a simpler definition: STS refers to the use of technology by people to carry out work tasks within an organisational context in order to achieve certain objectives. Table 2.13 lists some perspectives for Socio-Technical System Theory derived from previous studies.

The STS approach focuses on effectively using both the technological and human elements of organisational performance to achieve an optimal state of joint optimisation (Mumford, 2006).

Table 2.13 Socio-technical System Theory derived from previous studies.

Previous Research on Socio-technical System Theory	**References**
A classical socio-technical systems theory is a combination of the social and technical dimensions that are susceptible to their operating environments	(Appelbaum, 1997)
Socio-technical systems are distinguished by a high level of social intricacy and technical complexities intended to fulfil society's important functions	(Baxter & Sommerville, 2011)
They are the synergistic union of people, technology, organisational structures and processes, including the operating environment within which all these occur	(Carayon et al., 2015)
A socio-technical system is not one of two separate and side-by-side systems but the whole integrated system.	(Whitworth, 2009)
It is the interaction between the social (including how teams and individual team members perform tasks) and technical systems (including complex interdependencies of the system development life cycle)	(Troyer, 2016)
STS are made up of humans applying technology solutions to execute work activities through processes within a social structure (organisation) to accomplish set goals	(Bostrom & Heinen, 1977; Walker et al., 2007)
The social dimension is equally, if not more, complex even at smaller levels of groupings of people	(Troyer, 2016)
The technical dimension is mainly concerned with the provision of tools and techniques used to accomplish organisational goals	(Appelbaum, 1997; Egan et al., 2004)
Joint optimisation is the cornerstone and foundation of the socio-technical systems theory	(Susan & Mykletun, 2014)
STS approach is more concerned with harnessing the best of both the technical and human aspects of organisational performance to accomplish the joint optimisation state	(Mumford, 2006)
Where the joint optimisation state lacks, a socio-technical gap exists has cautioned that in reality, though, the relationships between people, processes and technology is more often non-linear (complex), recursive and difficult to predict.	(Troyer, 2016)
STS theory represents a unique approach relating to the interrelatedness of social and technical dimensions of an organisation	(Walker et al., 2007)
The STS theory provides a robust framework for the analysis	(Troyer, 2016)

The STS theory can provide a good framework for modelling organisations as complex systems	(Oosthuizen & Pretorius, 2016)
The social dimension consists of organisational structure and actors (including people). The technical dimension, on the other hand, comprises technology and work activities (tasks).	(Bostrom & Heinen, 1977)

Other scholars state that the socio-technical model encompasses four factors: culture, structures, methods, and machines (McEvoy & Kowalski, 2019), as seen in Figure 2.6. Machines are the technological tools used by the organisation. Methods include the techniques and processes used in connection to technology. The structure corresponds to the organization's setup, including both official and informal authority hierarchies. Culture describes the conduct shown by people and teams inside the organisation (Al Sabbagh & Kowalski, 2015).

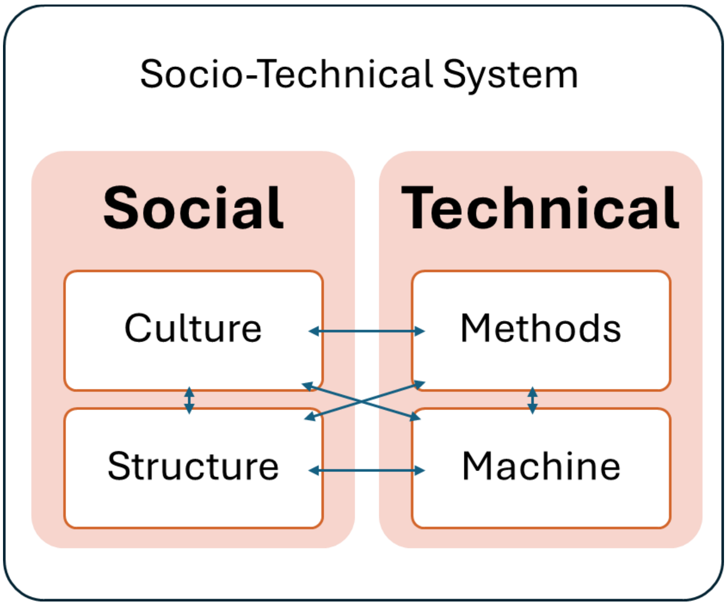


Figure 2.6 Socio-Technical System.

Irrespective of the complex nature of organisations that are complex technological and social systems, the STS theory offers a strong framework for analysis (Troyer, 2016). (Oosthuizen & Pretorius, 2016) argue that the STS theory offers a robust foundation for modelling organisations with complex systems. (Malatji et al., 2019) claim that the social dimension encompasses two key elements: the organisational Structure and the Actors involved, which includes individuals. In contrast, the technical dimension consists of two components: Technology and Work Activities (tasks) as shown in Table 2.14.

Table 2.14 Social and technical dimensions (Malatji et al., 2019)

Social dimension	Technical dimension
Structure	**Technology**
How the organization is arranged including both formal and informal authority structures	Tools and technology resources employed by the organization.
Actors	**Work Activities**
The behaviour of people, individuals and teams in the organization.	Tasks, processes and procedures used in relation to technology.
Environmental	
Stakeholders and External Entities	

(Clegg, 2000) revised the socio-technical principles to suit the modern age, focusing on meta, content, and process design. Clegg also introduced the hexagonal socio-technical framework, which is more relevant to this research. This framework was initially developed by Clegg in 2000 and has been further refined by (Davis et al., 2014). Figure 2.7 illustrates the hexagonal socio-technical framework and might present a FinTech business as a complex system consisting of socio-components (people, culture, and goals) and technical elements (technology, infrastructure, and procedures). (Clegg et al., 2017)

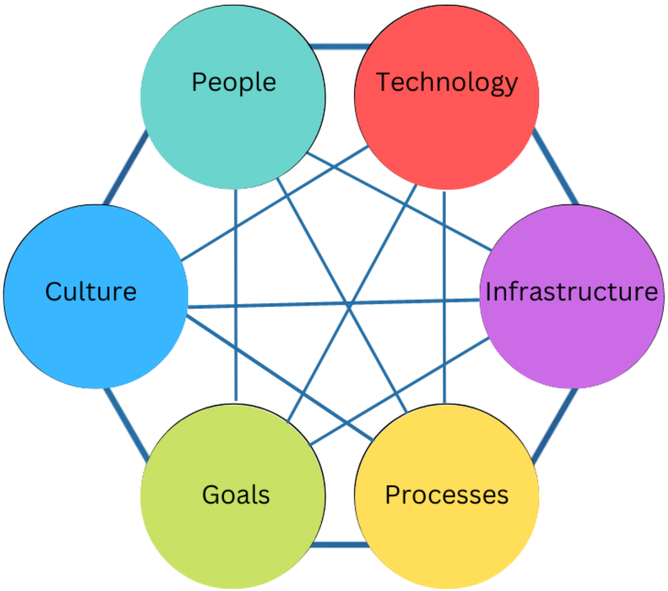


Figure 2.7 Hexagonal socio-technical systems framework - adapted from (Clegg et al., 2017)

2.12. Discussion and Analysis

The significance of a cybersecurity framework for financial institutions must be recognised. A cybersecurity framework acts as a collection of rules, policies, and procedures to handle cyber risks brought on by many highly advanced cyber threats. A cybersecurity framework places a strong emphasis on a scalable, adaptable, and economical method to stop cyber-attacks and boost the organisation's cyber resilience (Syafrizal et al., 2020).

Over time, there has been an unprecedented rise in the risk of cyber-attacks. It is important to understand that cybersecurity offers a financial institution several advantages, including company stability, increased return on investment, decreased risks, further business expansion, and alignment of business goals with information technology. Additionally, it makes financial institutions more resistant to cyberattacks (Kaur, Habibi Lashkari, & Habibi Lashkari, 2021; Knewtson & Rosenbaum, 2020; Schilirò, 2021; Turcan & Deák, 2021).

According to (Timeline of Cyber Incidents Involving Financial Institutions)'s report (Project, 2022), more than 200 cyber incidents targeting financial institutions since 2007 are becoming more frequent, sophisticated, and destructive. In 2017, the G20[1] warned that cyberattacks could "undermine the security and confidence and endanger financial stability." Based on the corresponding financial damage, the attack's severity was rated. It is crucial to note that these threats have been publicly disclosed. Since many cyber threats in the financial industry are never reported in favour of reputation and revenue loss, the actual figure is undoubtedly significantly high (Project, 2022).

The expense of repairing the harm brought on by cyberattacks is rising every day, as well. A cybersecurity framework provides the guidelines for monitoring cyber activities on the premises, designing preventive and detection methods, and taking necessary action to stop these activities in order to safeguard FinTech institutions from the threat of cyberattacks.

The cybersecurity framework should have characteristics that make it simple to implement and should not need huge resources or significant technical understanding. They should also be adaptable and customisable to FinTech's unique risk environment, security requirements, and skill level. Additionally, concerns are handled within financial contexts, resulting in easily understandable outcomes.

The choice to invest in adopting a particular standard should be carefully evaluated (Brotby, 2009). The assumption that a single standard would adequately cover corporate demands is unrealistic, given the difficulty of designing a generic high-level framework applicable to all FinTech company types. We were unable to locate any research that supports adopting a certain standard as a curative for all cybersecurity risk challenges. This is when a tailored approach may be the greatest option.

Although established cybersecurity standards have clear benefits, a rigid "one-size-fits-all" approach might expose FinTech organisations to vulnerabilities. Adhering to established standards is essential for establishing best practices and maintaining consistency, but there is value in acknowledging customisation. For example, the unique requirements of a healthcare provider will significantly vary from those of a FinTech institution. A generic standard may not sufficiently address the specific cyber threats encountered by each party. Customisation enables FinTech bodies to adapt security measures to their own business needs, regulation

[1] The G20 or Group of 20 is an intergovernmental forum comprising 19 sovereign countries, the European Union, and the African Union. It works to address major issues related to the global economy, such as international financial stability, climate change mitigation and sustainable development. Wikipedia

requirements, technology and systems' nature, and threat characteristics. By concentrating efforts on the most significant threats, this tailored strategy may enhance the overall security posture. Furthermore, customisation does not completely abandon existing standards. The goal is to use them as a starting point to develop a more robust and more adaptable security framework. When executed with careful consideration and expert involvement, customisation has the potential to enhance the quality and efficacy of FinTech's cybersecurity measures.

A customised approach leverages individual experience and transforms it into a solution that is matched with business needs. Rather than just relying on the standards' prescribed elements, FinTech firms might create their own inventory of threats, vulnerabilities, and risks unique to their business type. Additionally, associated controls and governance criteria must be tailored to FinTech's objectives and risk tolerance (Brock et al., 1999). A locally designed framework tends to grow and adapt over time while remaining closely aligned with FinTech business demands.

The research shows that several critical factors should be taken into account while developing a realistic cybersecurity framework for FinTech:

2.12.1. The Nature of Business

This covers the type of sector (financial, health, government, etc.) and size of the firm. Financial institutions face unique threats, vulnerabilities, and risks that telecom operators and hospitals do not (Syafrizal et al., 2020). Consequently, the cybersecurity framework varies for each business based on its characteristics, and the standards address these differences accordingly. The company's size directly influences the standard to be implemented. FinTech entities might consider using frameworks with simplified versions. Many standards, such as ISO 27001 and NIST, do not have simplified versions (Schlarman, 2007; Syafrizal et al., 2020).

2.12.2. Implementation Cost

This aspect might serve as a distinguishing feature when many frameworks satisfy FinTech needs, and their implementation costs vary. Usually, these implementations are done by consultants or third parties that charge hourly fees, but there are other costs to take into account as well. Extra costs consist of project management, necessary organisational changes and resources, awareness campaigns, and daily tasks to guarantee compliance with the set standard (Schlarman, 2007; Smith, 2019).

2.12.3. Required Skills

Not all frameworks need the same set of expertise for implementing and operating cybersecurity measures. Some frameworks need business experience, project management, and budgetary competencies, while others necessitate greater technical knowledge (Al Duhaidahawi et al., 2020). PCI DSS, for example, needs a higher level of technical skills than ISO 27001 or COBIT, which places a greater emphasis on business knowledge. However, PCI DSS controls are mainly focused on credit card transaction-specific defences rather than general cybersecurity. Maintaining a firewall to secure cardholder data, encrypting credit card transfers, limiting access to cardholder data, and routinely testing security systems and procedures are a few examples of PCI DSS measures (Smith, 2019).

2.12.4. Comprehensiveness

While designing a cybersecurity framework for FinTech, it is critical to keep in mind that the framework should include all necessary features and details rather than just cover the subject in general. Comprehensiveness is another factor to consider since it reflects the extent to which the framework provides coverage (Syafrizal et al., 2020). ISO 27001 is a generic standard for risk management in information security, in contrast to ISO 27005, which is a security-specific standard. ISO 27002 does not provide a thorough list of all controls that must be implemented, although NIST does (Knapp, 2009; Schlarman, 2007; Syafrizal et al., 2020). The development of a realistic and systematic cybersecurity framework for FinTech is a future challenge (Abdullah et al., 2018; Basole & Patel, 2018; Eickhoff et al., 2017).

2.12.5. Regulations

The emergence of FinTech enterprises and the fundamental transformations they have brought about on a wide range of fronts, including how banking operates, how capital is sourced, and even the very nature of money itself, have not been adequately accounted for by regulation (Magnuson, 2018). Moreover, it is critical to emphasise that financial-sector regulators' activities must be coordinated with national cybersecurity plans and frameworks. This relationship is maintained by continual communication with relevant national entities, including but not limited to government, national intelligence, and law enforcement authorities (Panetta, 2018).

In Bahrain, in order to encourage effective use and trust in new technologies, assist finance-related concerns, and enhance the customer experience with FinTech, the CBB firmly decided to establish the regulatory Sandbox. These regulations safeguard customers and promote market anti-money laundering. The CBB set the Sandbox's duration at nine months, with a possible extension of three months, with the following qualifications: innovation, customer benefit, technical testing, readiness for regulatory testing, and deployment post-testing (Ali et al., 2021). However, no criteria are clearly mentioned concerning the cybersecurity of these FinTechs and their measures to ensure customers' data protection and infrastructure security.

In order to effectively address the distinct challenges and risks inherent to Bahrain's FinTech sector, it is imperative to develop a comprehensive national cybersecurity strategy. The strategy should include specific goals, governance structures, risk management procedures, and incident response plans. Improving cybersecurity in the financial sector also requires collaboration amongst stakeholders, including FinTech companies, financial institutions, regulators, and governmental authorities. To effectively tackle common risks and vulnerabilities, policymakers should promote information exchange and the use of standard procedures. Additionally, regulators should establish precise criteria for cybersecurity risk assessments, third-party risk management, and incident reporting, and FinTech companies should adhere to relevant regulatory standards and norms linked to cybersecurity. Furthermore, policymakers could encourage FinTech companies to invest in cybersecurity by offering cybersecurity training and education to assist companies in establishing a cybersecurity culture and putting effective security measures in place. Ultimately, to guarantee that their cybersecurity plans are current and successful, regulators should keep a vigilant eye for new risks and vulnerabilities in the FinTech field through continuous research and analysis.

Although a variety of approaches for addressing cybersecurity challenges in FinTech have been established (Suryono et al., 2020), none of them take into account the weakest link, which is the human factor that might be exploited by cyber-attacks. Furthermore, the papers examined do not approach cybersecurity from a sole management standpoint but rather from an IT perspective.

Al-Ahmad & Mohammad, (2012) interpret that standard certification does not always imply that a FinTech is secure(Al-Ahmad & Mohammad, 2012). If not maintained appropriately, cybersecurity certifications might create an illusion of security. Additionally, since the standards are pretty system-oriented, excluding organisational factors, there is a scarcity of a comprehensive view of cybersecurity risk management. High implementation costs, a lack of qualified professionals, and the generality of standards extend to all of the previously listed factors (Al-Ahmad & Mohammad, 2012). The generality of the standards does not account for variances in business risk needs, which might lead to different definitions by different stakeholders. The complexity of cybersecurity frameworks is restricting their acceptance in certain businesses that lack the skills and resources to implement them (Kaur, Habibi Lashkari, Habibi Lashkari, et al., 2021). To solve this issue, a light version is recommended that may be utilised as a starting point for many SMEs and FinTech companies. It may also be used by businesses as a baseline for achieving a suitable degree of security control and governance (Al-Ahmad & Mohammad, 2012).

The findings of the SLR thematic analysis indicate that the constraints of FinTech research begin with identifying the FinTech framework (Basole & Patel, 2018; Eickhoff et al., 2017), which includes business models and models tailored to each organisation's culture. These factors have a significant impact on national regulations and policies (Davis et al., 2017; Gomber et al., 2017; Hung & Luo, 2016; Suryono et al., 2020). This sector necessitates conceptual frameworks that must be adjusted to technology advancements (Suryono et al., 2020). As a result, numerous countries have implemented the regulatory sandbox approach (FinTech start-up incubation), as seen in Singapore and Bahrain (Abdelghani et al., 2021; Al-Shakar, 2017; Haddad & Hornuf, 2019; Mehrotra, 2019). FinTech demands a lot of personal data; therefore, keeping an eye on the platform is also important for consumer data protection (Stewart & Jürjens, 2018). The standard of data protection and infrastructure security must be regularly improved on this basis (Syafrizal et al., 2020). FinTech companies are now obliged to work with conventional financial institutions such as banks.

Technology adoption may be considered in the area of information systems, including merging user acceptance models with other behavioural models (Abdullah et al., 2018; Albastaki & Manta, 2020; Schierz et al., 2010; Stewart & Jürjens, 2018; Wang et al., 2015; Wonglimpiyarat, 2017; Zavolokina et al., 2016). Collaboration with other businesses on the FinTech business model is also conceivable (Suryono et al., 2020). It's also possible to assess the technology's maturity and, create technical and non-technical recommendations, and review policies to develop regulations that are acceptable to stakeholders and in line with the FinTech systems (Smith, 2019). FinTech must also be considered part of education to prepare prospective employees for the market (Mehrban et al., 2020).

2.13. Summary

This chapter discussed the existing cybersecurity issues in the FinTech industry in Bahrain, employing a structured approach to the literature review and qualitative analysis of the inclusions of the articles that were chosen. The SLR assessment of the articles focused on three areas of analysis in particular:

1. A review of the FinTech and cybersecurity concepts and definitions.
2. Cybersecurity countermeasures, guidelines, standards, and frameworks.
3. There is a need to develop a cybersecurity framework for FinTech entities in Bahrain.

The primary goal is not to start from scratch but rather to make use of what has already been accomplished and learned in the field of cybersecurity framework and standards. However, our review includes some components of cybersecurity standards that haven't previously been considered with regard to FinTech innovations.

This chapter uses a reproducible method to gather and synthesise scientific community-proposed cybersecurity frameworks and FinTech to determine the research gap in Bahrain. It answers the research questions by highlighting the cyber threats facing FinTech firms. From the literature, there are several countermeasures to address these challenges, including a comparison review of regulatory frameworks and existing cybersecurity standards. This review encourages cross-pollination among research methodologies and provides suggestions for prospective cybersecurity frameworks for FinTech businesses in Bahrain.

Recognising the scope and importance of this study, it is essential to consider any constraints that may affect the clarity and applicability of the results. Firstly, the lack of a specific quality evaluation in the chosen studies poses a possible risk to the general validity of the research. Although the PRISMA technique was used for systematic review, the absence of a comprehensive evaluation of the quality of the articles included adds variability that has to be taken into account. Authors must identify the limitations arising from this exclusion and recognise that the variable quality of the examined studies may impact the robustness of the derived results.

Additionally, an important limitation arises from the continuous development of recent studies on the research topic and in the FinTech and Cybersecurity fields following the initial search for articles.

The last part of the chapter laid the groundwork for the theoretical framework in this research by exploring the historical development of STS theory, tracing its origins from the seminal work of researchers. It reviewed the existing literature that has employed the STS framework to study complex organizational and technological systems, highlighting key concepts, models, and empirical findings and examining the complex interplay between technology, people, processes, and the environment in the FinTech systems. FinTech as a complex socio-technical system was presented, and the current body of research on cybersecurity concerns in this industry was explored. By analysing the interaction of various aspects, the chapter established the foundation for comprehending the complex nature of cybersecurity threats in the FinTech industry.

This page intentionally left blank

Chapter 3: Research Methodology

3. Chapter 3: Research Methodology

3.1. Introduction

As discussed in the previous chapter, FinTech firms, in general, require a robust cybersecurity framework to control both their business and technical operations. Determining the research problem is essential since it helps determine the study objectives, which in turn influences the steps that come next in terms of collecting data and the method by which the data is analysed (Creswell & Creswell, 2017). In order to aid in the selection of research techniques and methodology, it is also essential to clarify the link between the research question and its objectives. It provided a detailed explanation of the STS-informed research design, including the rationale for selecting the ideal research method approach.

This chapter will go through the research methodology and the in-depth discussion of the detailed research philosophy used to achieve the defined objectives of the study. Moreover, the research approach, research design, study population, sampling, research instrumentation, and data collection and analysis techniques will all be covered as well. Furthermore, this research will clarify the underlying limitations, constraints, and ethical implications associated with it.

3.2. Research Philosophy

The research philosophy pertains to the study's nature, assumptions, and knowledge. It deals with how knowledge is developed. This matter should be taken into account because various researchers may hold different beliefs regarding the nature of knowledge and truth, and philosophy helps us understand these beliefs (Tsang, 2016).

It is essential to clearly articulate the research philosophy used in this study. The research philosophy options available for consideration include pragmatism, positivism, realism, and interpretivism (Patten, 2016). These philosophies will be further elaborated upon in the subsequent discussion. Moreover, it is vital to provide the rationales behind the philosophical categorisations of the topic of study (Tsang, 2016). This chapter will go into the discussion around the impact of research philosophy on research strategy as a whole, as well as its influence on the selection of primary data-collecting methods.

Research philosophy addresses the origins, characteristics, and development of knowledge (Williams, 2007). In simple words, research philosophy is a view of how information about a phenomenon should be gathered, examined, and applied.

While the concept of creating knowledge may seem broad, it is essential to acknowledge that going through this research is actively involved in the process of knowledge creation. Primary and secondary data are gathered and analysed in order to respond to the research question and provide new knowledge. Furthermore, addressing research philosophy essentially entails identifying and articulating research assumptions and views. (Saunders et al., 2016) identified research philosophy is located at the outer layer of the "Research Onion", as shown in Figure 3.1

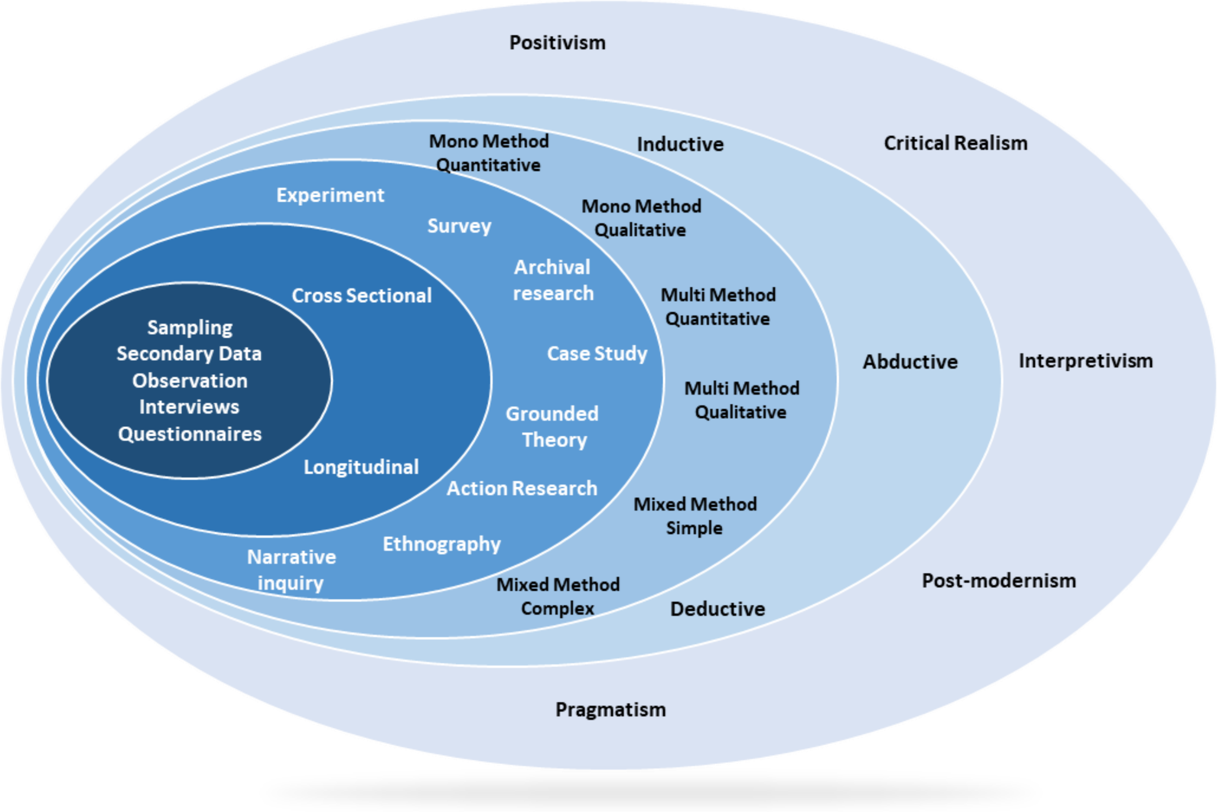


Figure 3.1 Research Onion - (Saunders et al., 2016)

Practical considerations influence the selection of a particular research philosophy. Significant conceptual distinctions exist between quantitative studies and qualitative research. The choice between positivist and interpretivist research philosophies, as well as between quantitative and qualitative research methodologies, has historically been a significant topic of argument (Creswell & Creswell, 2017). Nevertheless, recent advancements in research methodologies (Mbanaso et al., 2023) have led to a surge in the adoption of pragmatism and realism philosophies. Additionally, Table 3.1 provides a comparison of research philosophies, their advantages, disadvantages, and related data collection methods for each philosophy (Oates et al., 2022).

Table 3.1 Research philosophies and data collection methods - (Oates et al., 2022)

Philosophy	**Focus** In Computer Science	**Advantages**	**Disadvantages**	**Data Collection Methods**
Pragmatism	Focuses on practical applications and solving real-world problems. Aligns with the goal of developing helpful computing solutions.	- Guides development of effective systems. - Encourages user-centered design.	- Relies heavily on context, making results less generalizable. - Subjective evaluation can be prone to bias.	- User studies - Case studies - Action research
Positivism	Emphasizes objective, measurable data and scientific methods. Common approach in computer science for evaluating algorithms and systems.	- Provides rigorous and replicable research. - Quantitative data allows for statistical solid analysis.	- Limited view of reality, neglecting subjective experiences. - Can be difficult to isolate variables in complex systems.	- Experiments - Surveys - Observational studies with structured data collection
Realism	Assumes there is an objective reality that can be discovered through research. Underpins the development of theoretical models in computer science.	- Provides a foundation for understanding the underlying principles of computing. - Helps validate theoretical models against real-world phenomena.	- Can be slow to yield practical results. - Difficulty in directly observing and measuring some aspects of computing systems.	- Mathematical modelling - Simulations - Experiments with controlled environments
Interpretivism	Focuses on understanding the meaning people give to their experiences with technology. Useful for studying human-computer interaction and user experience.	- Provides insights into user behaviour and motivations. - Informs the design of user-friendly interfaces.	- Relies heavily on qualitative data, making results difficult to quantify. - Subjectivity of interpretation can lead to conflicting viewpoints.	- Interviews - Focus groups - Ethnographic studies - Document analysis

Pragmatism allows for a practical and problem-solving approach, which is suitable for developing a cybersecurity framework that addresses the specific needs and challenges of the FinTech industry. (Mbanaso et al., 2023) show how the pragmatist approach can be applied in the fields of computer science, information systems and cybersecurity. A pragmatist approach can facilitate the development of a framework that effectively balances security concerns with business realities, which prioritises practical solutions and real-world results (Williams, 2007).

Cybersecurity standards were designed to provide comprehensive protection against all prospective threats. Nevertheless, a pragmatic approach emphasises the most possible and significant threats that FinTech companies face (Tsang, 2016). These specific risks would be prioritised by a pragmatic approach in terms of controls. Additionally, a pragmatic approach points out the importance of utilising existing solutions rather than reinventing the wheel (Wohlin et al., 2012). A robust foundation is provided by established security frameworks, such as the NIST Framework. This approach offers a foundation for the FinTech industry's specific threat landscape, while also facilitating customisation.

Therefore, the pragmatism research philosophy, which enables a realistic and solution-oriented methodology, is well-suited for this research. It can be used to develop a cybersecurity framework that effectively caters to the unique needs and challenges encountered within the FinTech sector in Bahrain.

3.3. Research Approach

The chosen research approach will include the use of both deductive and inductive reasoning. The process of deductive reasoning involves getting started with existing standards and frameworks relating to cybersecurity and then adapting and applying them to the domain of FinTech. The use of inductive reasoning would be employed to collect empirical data and get insights from the FinTech experts in order to refine and validate the framework.

The study analyses a significant number of previous studies on the rise of FinTech innovations worldwide and in Bahrain and assesses the impact of cyber threats on these businesses. The results from previous research, along with newly gathered data, are used to identify the fundamental principles of the proposed cybersecurity framework for Bahrain’s FinTech stakeholders.

3.4. Methodology Approaches

The selection of a research design is determined by the methodological option made to address the research question. According to (Saunders et al., 2016), social research may be categorised into three main approaches: quantitative, qualitative, and mixed methods. One of the notable advantages of qualitative research, as highlighted by (Harper, 2013), is its capacity to direct attention towards real-world practises, therefore examining the regular functioning of organisations. Moreover, qualitative research enables scholars to comprehensively investigate complex phenomena. One of the primary objective of this study is to collect comprehensive and complex data pertaining to the experiences, views, and behaviours of the participants. This approach facilitates the exploration of many aspects of a study subject, leading to a thorough comprehension of the fundamental factors, interpretations, and contexts involved (Dawadi et al., 2021).

(Bazen et al., 2021) emphasise that qualitative research offers the unique advantage of examining subjective experiences and perspectives. Through open-ended questions and in-depth interviews, researchers can explore individuals' thoughts, feelings, and motivations, providing valuable insights into their worldviews. This deep exploration of personal narratives allows for a comprehensive understanding of the underlying factors that drive behaviours and decision-making processes.

Furthermore, it facilitates the generation of novel theories, conceptual frameworks, and new perspectives via the exploration and analysis of unexplored fields (Rahman et al., 2021). Open-ended interviews, focus group discussions, observations, and content analysis can facilitate the exploration of diverse viewpoints and the construction of theoretical frameworks (Keenan, 2015). (Sachdeva, 2019) reveals that qualitative research provides a high degree of flexibility and adaptation throughout the whole of the research endeavour. Researchers can enhance the precision of their research plans, modify their techniques, and investigate emerging patterns while doing data collection and analysis.

Considering all the above features of the qualitative method, this study aligns with this approach.

3.5. The Socio-Technical Systems Theory

When considering the philosophical approach of this study, it is essential to also give a philosophical explanation of the chosen socio-technical systems STS theory.

(Ropohl, 1999) defines socio-technical systems as a theoretical framework that provides a description and explanation of technology evolution. Initially, the technological circumstances at work must align with both humanity and efficiency without any contradiction.

Ropohl used systems laws to analyse an action system, which is seen as a socio-technical production system. This analysis aims to characterise the social and technical phenomena, including people and machines, as well as the process of technology being integrated into society and society becoming influenced by technology. (Al Sabbagh, 2019)

The STS theory was employed to develop a theoretical framework for examining organisational activities in relation to their social, technological, and environmental impact on FinTech companies. Subsequently, the theoretical framework was used to analyse and align with some cybersecurity standards. The result of this exercise led to the establishment of main themes for a cybersecurity framework that can be used for FinTech's business environment.

3.5.1. Framework Development Methodology

Our approach optimises risk analysis and management by combining socio-technical and human factor analysis to identify threats. However, it should be noted that our approach is not a comprehensive methodology but rather a secondary approach. For instance, ISO27001 is a comprehensive framework that is used to guide the selection of risk analysis procedures [21]. It illustrates the sequential steps involved in the process of risk analysis and management, which may be further subdivided into many activities. We consider our approach as a risk identification instrument. The technique enables the identification and incorporation of different risk elements, such as threats, vulnerabilities, or effects, into an extensive investigation in conjunction with other research.

The process for developing a cybersecurity framework is shown in Figure 3.2 and includes the following steps:

1. Conduct an analysis of STS theory and construct a theoretical framework. The socio-technical systems theory is examined, and a comprehensive theoretical framework is developed that highlights the important factors to pay equal attention to both the social and technological dimensions.

2. Evaluate cybersecurity controls using the theoretical framework. The evaluated controls (attributes) were in accordance with the published and industry-recognized cybersecurity frameworks.

3. Create STS cybersecurity themes. The security measures are examined and systematically evaluated using the theoretical framework, and then assembled. This results in the emergence of innovative and flexible advanced cybersecurity themes.

4. Conduct a qualitative data collection and analysis that aligns with the theoretical framework.

5. Develop and set up the cybersecurity framework. Develop cybersecurity principles and controls for the proposed cybersecurity framework.

6. Validate the integrity and effectiveness of the cybersecurity framework.

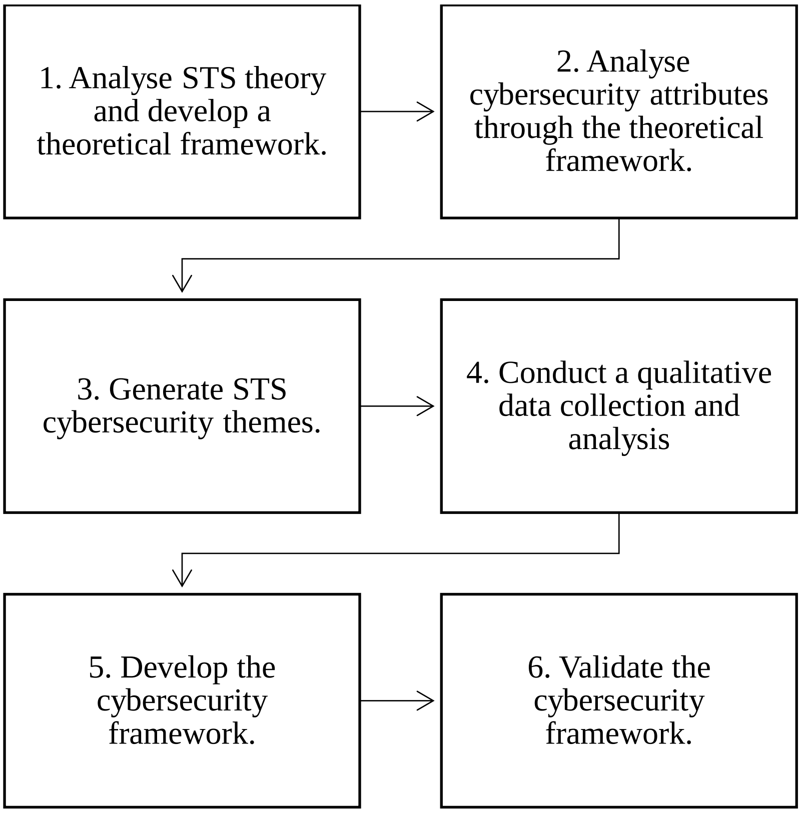

1. Analyse STS theory and develop a theoretical framework.
2. Analyse cybersecurity attributes through the theoretical framework.
3. Generate STS cybersecurity themes.
4. Conduct a qualitative data collection and analysis
5. Develop the cybersecurity framework.
6. Validate the cybersecurity framework.

Figure 3.2 Framework Development Methodology.

3.5.2. Theoretical Framework

Based on the STS theory review in Chapter 2, Table 3.2 acts as a reference for conceptualising and developing the essential attributes for both the social and technical elements of an STS within a complex environment like the FinTech ecosystem (Malatji et al., 2019). Table 3.2 indicates that:

Organizational structure plays a crucial role in facilitating authority, communication, and workflow. (Hester, 2014) defines actors as all members of a complex STS, including key stakeholders who affect or conduct work activities. Technology equips workers with tools and resources to do jobs. Work activities occur inside social infrastructures, including government rules and regulatory frameworks.

(Malatji et al., 2019) Emphasise the interaction between attributes within each element and across the STS framework. For example, FinTech organisational structure includes elements such as reporting hierarchies, management support, and human resources system. These aspects are essential in determining the overall operation of FinTech. Technology, however, offers the resources and tools that people, inside the FinTech firm, use to carry out their job duties. This encompasses several components such as hardware, software, devices, network, and IT policies. The type of technology used has a considerable impact on the specific skills and expertise staff members need. For instance, the utilisation of sophisticated data analysis technologies may need the recruitment of people with competent data visualisation skills. Actors consist of people, teams, and the interactions among them. Moreover, actors, including external entities like as vendors, customers, and potential stakeholders, have a vital impact on moulding the social aspect through their interactions and partnerships. Work activities encompass the precise responsibilities and their organised tasks. Examining these attributes is essential for comprehending the process of work execution inside FinTech organisation. The environmental dimension, encompassing political and legal considerations, might potentially affect the reporting structures and authority within the organisational dimension.

Table 3.2 Social and technical dimensions attributes (Malatji et al., 2019)

Social dimension	**Attributes**	**Technical dimension**	**Attributes**
Organisational structure (functions)	Skill/ability Values and norms Patterns of behaviour Culture Knowledge reporting/authority Structures and control Reward systems Coordination needs Policy	**Technology** (tools/resources)	Hardware Software Equipment Machines Tools Physical security Cybersecurity Built environment Information Processes Procedures Techniques
Actors (human beings)	Individuals/people/humans Teams/work groups	**Work activities** (tasks)	Activity tasks Work organisations

	People relations		
Environmental dimension			
Political Economic Social Technological	Environmental Legal Geographical locations Natural disasters	Built environment Physical environment Suppliers Customers	Government Other external entities

3.6. Research Gap

Although several cybersecurity frameworks have been reviewed in the literature, no framework fully addresses other critical factors concerning cybersecurity threats to financial organisations, such as end-user culture, awareness programmes effectiveness, integration with existing laws and regulations, and staff competency level of cybersecurity. Based on this outcome, by the end of this research, we will propose a framework that can be used as a cybersecurity assessment tool for FinTech entities of Bahrain that integrates all security and privacy regulations and best practices with which this FinTech must be compliant. Such a framework can be used as a gap analysis tool as well as an inspection mechanism, enabling FinTech firms to gain detailed compliance reports and statistical analyses of their security posture.

Several factors and research areas are identified to develop a cybersecurity framework for FinTech. From the literature, the following are the common factors that need further focus in this study, which in turn represent the common areas in the STS theoretical framework:

- Risk - *Structure*.
- Processes – *Work Activities*.
- Technology - *Technology*.
- People - *Actors*.

In addition, several concerns and challenges affecting the robustness of the cybersecurity framework for FinTech need to be explored, such as regulations and third parties, in the environmental dimension.

3.7. Research Main Question

A research question refers to a precise inquiry or problem statement that provides direction for a research investigation. The statement defines the topic of study or concern that will be explored and establishes a clear focus for the research process. The formulation of a research question plays a crucial role in assisting researchers in establishing the scope of their study, identifying the most suitable research methodologies, and guiding the process of data gathering and analysis (Keenan, 2015).

The primary focus or subject of inquiry that the researcher intends to examine is emphasised through the following question:

What are the crucial elements in developing a Cybersecurity Framework designed for FinTech entities in Bahrain?

The research question is extended into the following research objectives and more detailed research questions.

3.8. Research Objectives and Methods

Specifically, within the context of Cybersecurity for FinTech, the objectives of this research were listed in section 1.7 of chapter 1. These objectives will be investigated and achieved via the following research methods listed in Table 3.3:

Table 3.3 Research Ojectives

Objectives	Description	Methods	Chapters
Objective 1	To review significant risks facing FinTech innovations within Bahrain's financial sector and security monitoring tools used for interpreting malicious activities.	SLR	**2**
Objective 2	To determine what governance elements are in place addressing FinTech systems protection.	SLR	**2**
Objective 3	Data collection by interviewing experts to investigate the incident response plans, vulnerability management, and prevention actions in case of any compromised system, and to evaluate end user's behaviours and skills	Semi-Structured Interviews	**4**

	in the context of cybersecurity, and what education, training, and awareness reinforcement are needed.		
Objective 4	Analysing the collected data to develop a cybersecurity framework for FinTech in Bahrain. A framework that can be shared seeking for assuring cybersecurity in all FinTech entities consistently yet appreciates the differences in business environments.	Qualitative Analysis using STS Theory and Le Compte Model	**4**
Objective 5	To validate the proposed cybersecurity framework and test its applicability.	Focus Group & Delphi Session	**5**

3.9. Research Design

The research strategy provides a plan to find answers to questions throughout the research. It specifies the research's main questions, the type of research, data gathering techniques, and the strategy suggested for qualitative analysis. The design is considered a model for the conceptual research structure, which helped to establish participant group levels and data-collecting methods (Rovai et al., 2013). The research design will be exploratory in nature as it aims to understand the current cybersecurity practices and challenges in FinTech innovations. Additionally, conclusive research would be carried out to create and validate the cybersecurity framework.

3.9.1. Secondary Data

STS theoretical framework was employed in this research to provide the foundation for connecting risk, people, processes, and technology to develop a cybersecurity framework for FinTech.

Moreover, other secondary data is derived from literature resources, which include comparative analysis in publications such as journal articles and white papers on the well-known cybersecurity standards. This will provide additional insights into cybersecurity controls for the financial sector. Other documents include rule books, reports, and regulations published by the Central Bank of Bahrain (CBB), Information and eGovernment Authority (iGA), National Cyber Security Centre (NCSC), and national stakeholders concerning cybersecurity in the financial industry. Only credible and relevant materials were considered.

3.9.2. Primary Data

Primary data was collected through semi-structured interviews with financial institute employees, executives, and FinTech experts in Bahrain. The use of qualitative research techniques will result in a deeper understanding of the framework's key principles and satisfy the research's objectives. It is important to align the research design with the research questions that need to be examined (Williamson, 2004).

The data collection methods would include a qualitative approach. Qualitative methods such as interviews and focus groups would be used to gather insights and perspectives from cybersecurity experts and professionals in the FinTech domain. Figure 3.3 depicts the research design and plan and corresponding chapters in circles.

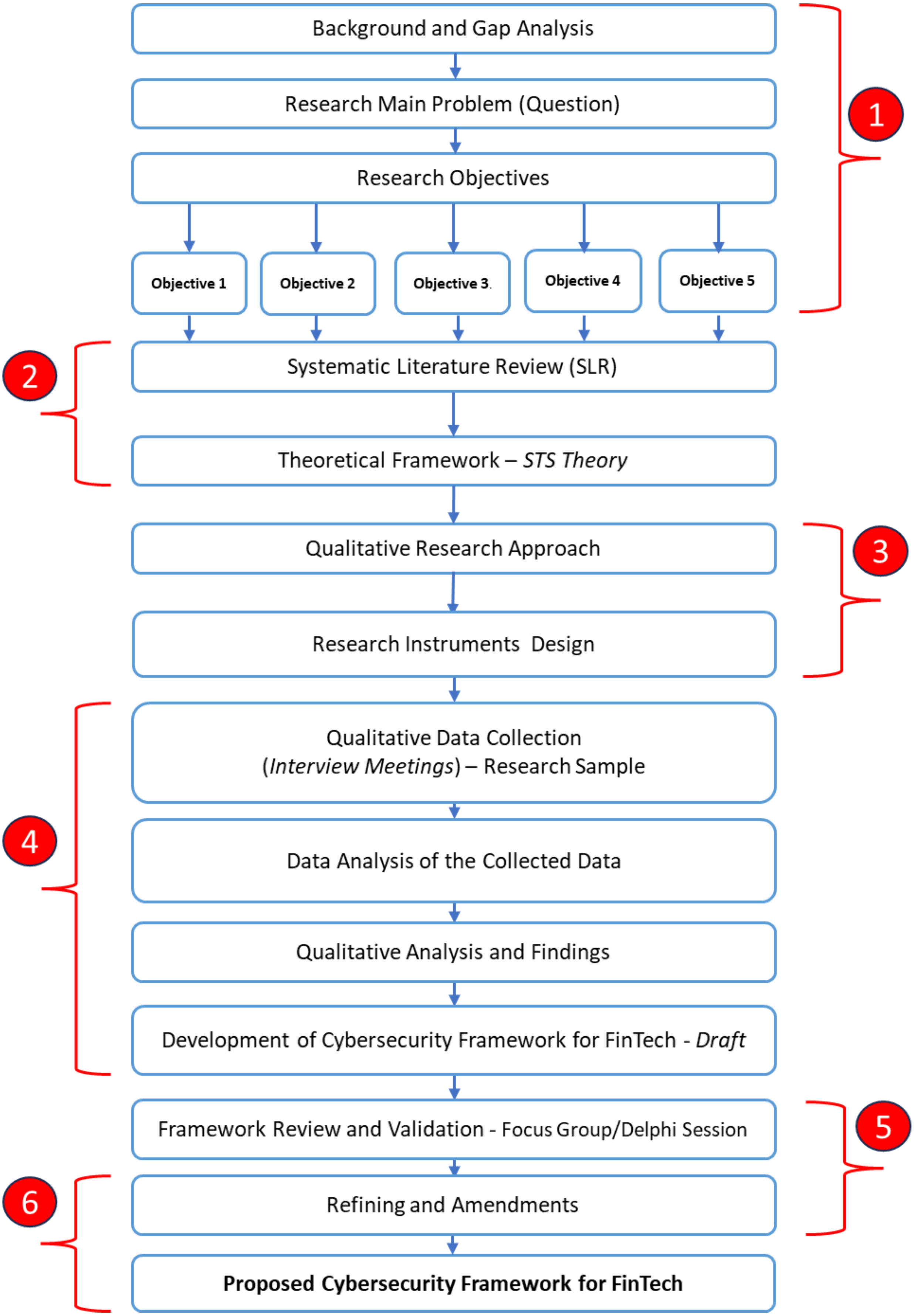

Background and Gap Analysis
Research Main Problem (Question)
Research Objectives
Objective 1
Objective 2
Objective 3
Objective 4
Objective 5
Systematic Literature Review (SLR)
Theoretical Framework – STS Theory
Qualitative Research Approach
Research Instruments Design
Qualitative Data Collection (Interview Meetings) – Research Sample
Data Analysis of the Collected Data
Qualitative Analysis and Findings
Development of Cybersecurity Framework for FinTech - Draft
Framework Review and Validation - Focus Group/Delphi Session
Refining and Amendments
Proposed Cybersecurity Framework for FinTech
1
2
3
4
5
6

Figure 3.3 Research design and plan and corresponding chapters in circles.

3.10. Research Instruments

As mentioned in the preceding section, the interview questions instrument is used to conduct this study. Following the question planning steps by (Brancato et al., 2006), the interview questions are created in a semi-structured way. Figure 3.4 shows those stages.

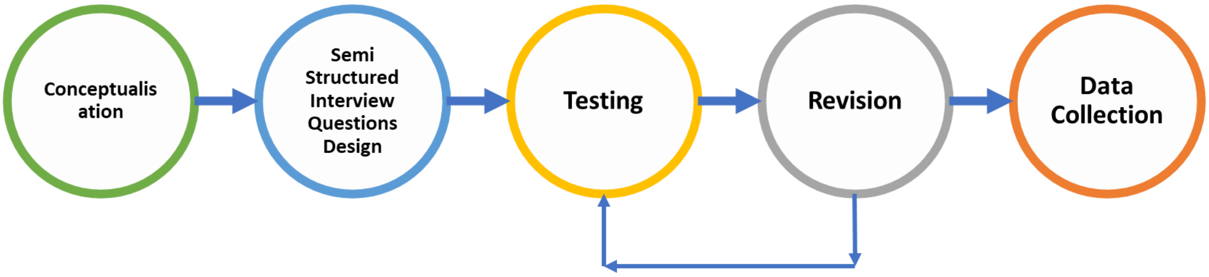


Figure 3.4 Question Planning Steps (Brancato et. el 2006)

To start, the study questions and associated objectives were developed based on the examination of the research problem provided in the literature review in Chapter 2. As a result, the researcher began to compile a list of possible questions that should be addressed. Each research objective is linked by a series of questions. The questions were then screened, and the best-fit ones were used to develop the final interview questions (Appendix 2). It was essential to make the questions simple to complete and quick to answer since participants often avoid lengthy and complex questions.

3.10.1. The Interview Sessions

Interviews with experts are conducted to supplement the data gathered in this study. The interview survey will aid in gathering qualitative data for analysis. The interview will assist in obtaining a first-hand impression of the specialists who were chosen for this research. The interview techniques have been designed systematically with comprehensive coverage of research objectives to address the research questions posed by the review of literature compiled and analysed in Chapter 2.

Because the interviewed experts would have limited time and will cover various topics depending on their knowledge, the interview instrument separated each objective with a few questions.

3.10.2. Guided Interview Questions

Although there are only 10 interview questions, these were designed to obtain their broad view of the financial industry's cyber risks and countermeasures to address them as a consequence of the emergence of FinTech service providers. Table 3.4 lists guided questions asked/discussed during the interviews.

Table 3.4 Interview Questions

	Interview Questions	Theme
1.	What IT assets do you think are most vulnerable to cyber-attacks? What are cyber threats targeting your organisation?	Cyber Risks
2.	Which cybersecurity standards/framework your institution is committed to? What are the reasons for selecting this option?	Regulations and Policies
3.	Where do you think your company is in terms of the maturity of your Cybersecurity strategy?	Regulations and Policies
4.	Which regulatory/compliance issue(s) would be of concern if firms were to collaborate with other FinTech companies?	Regulations and Policies
5.	What are the security technologies and solutions to protect against cyberattacks?	Level of Technology
6.	What types of security monitoring and protection tools are used for interpreting malicious activities?	Level of Technology
7.	What challenges do you face in implementing a cybersecurity protection solution?	Level of Technology
8.	What barriers inhibit your organisation from adequately defending against cyber threats?	Cybersecurity Operational Processes
9.	What education, training, and awareness reinforcement are needed to improve end users' behaviours and workers' skills in the context of cybersecurity? What are the most critical security skills required in your organisation?	Cybersecurity Awareness and Capacity Building
10.	Should the government get more involved in helping to combat cyber threats in a systemically important industry like banking/financial services?	Third Parties and Other Stakeholders

3.10.3. Research Instrument Clarity and Pilot Testing

The interview questions were written in simple and precise language to ensure its clarity and that the participants could answer it. In addition, the terms chosen were appropriate for the intended sample's level. After the interview questions were ready, they were reviewed with the supervisor several times. Upon receiving confirmation on the final question sets, a pilot test was performed to obtain input on the usability and practicality of completing the interview questions.

Pilot studies are valuable techniques that serve as a preparatory step for an in-depth interview. It can be utilised to fix possible shortcomings that arise in the following research process and offer a testing exercise of the questions. It can assist in identifying any weaknesses or limitations in the interview design that may require necessary modifications. The objective was to evaluate the suitability of the questions and give the researcher initial insights into the feasibility of the interview procedure. In addition, it also enabled researcher to gain experience in conducting semi-structured interviews and establish a strong communication skill with participants who will contribute knowledge. In addition, it facilitated the researcher's development of interviewing capabilities and the flow of discussion.

Permission sought to engage the professionals from one local FinTech company. A formal email was sent to the company's personnel representative and the researcher shared a similar criterion to the potential participants for the actual research. A respond approval was obtained, and two employees were identified from the FinTech company. It signified that the participants were selected based on purposive sampling and willingness to participate and an effort was made to interview one cybersecurity expert (male) and one female professionals from regulation and compliance department.

Following the pilot interviews, the interview techniques were enhanced. Conducting a pilot of the interview questions was extremely beneficial, as it allowed necessary modifications to be made before conducting the main interviews. Several questions were revised and structured sequentially, while others were reviewed and merged to enhance the quality of data collection and generate more in-depth responses from the participants. The modified version was shared and reviewed with the supervisors before being submitted to the ethics panel for final approval.

3.10.4. Academic Ethics

As per the University of Salford guidelines, any research activity needs ethical consideration. No field work, experimentation, or work with participants (directly or indirectly) can start until approval is granted. The Academic Ethics Policy outlines the expectations and requirements for all students conducting academic activities at, or on behalf of, the University of Salford. Following the university's guidelines and procedures, the researcher has submitted an ethics application, and approval has been granted by the ethics committee. (See Appendix 5: Ethics Approval)

3.11. Data Collection Method

The data collection method for this study is guided by the theoretical framework of socio-technical systems (STS), as discussed in Chapter 2. The STS model approach was adopted to ensure a comprehensive understanding of the research context, encompassing both the social and technical aspects. As previously stated, the research uses a qualitative data collection method. The goal of this approach is to get a better comprehension of the data and draw clear conclusions. For qualitative data collection, interviews were scheduled with certain main stakeholders from financial institutes and FinTech companies to get deeper and broader knowledge from technical experts. Board and executive management members, IT management and process owners, risk, compliance, and legal specialists, IT auditors and consultants, and regulators' experts caring about cybersecurity for FinTech are among the interviewees. The interview questions were designed to obtain a broad view of the financial industry's cyber risks and countermeasures to address them as a consequence of the emergence of FinTech service providers. Furthermore, it was used to gather in-depth insights into the social dynamics, organizational structures, and cultural factors influencing FinTech’s socio-technical systems.

Although there were several interview questions, there was a time restriction in obtaining appointments with the interviewees due to their extremely busy schedules.

3.11.1. Population of the Study

A population refers to the comprehensive collection of individuals and cases that belong to a particular class or interest group, sharing a defined set of common characteristics (Suri, 2011). Population is used as a means for identifying the whole from which the sample is selected (Williams, 2007). The research population for this study comprised executive leaders, IT managers, risk, compliance, and legal specialists, cybersecurity auditors and consultants, and Information security and IT specialists who had a part in business operations, regulatory, or compliance activities inside Bahrain financial institutions. These individuals, as shown in Table 3.5, were approached for the purpose of data collection (interviews) and were the target group for this qualitative research.

3.11.2. Research Sample

Qualitative research places significant emphasis on the deliberate selection of participants who possess relevance to the study problem, possess distinctive viewpoints, and have the capacity to provide comprehensive and varied insight (Saunders et al., 2016). The determination of sample size in qualitative research is guided by the principle of data saturation (Williams, 2007). This approach entails terminating the process of data collection and analysis when little or no new information or themes arise from the data. Scholars continue gathering data until they reach a state of conceptual saturation when the acquisition of more evidence is unlikely to provide significant novel findings. To meet the study needs of a justified sample with particular criteria, the approach of (Purposeful Sampling) was used. Purposeful sampling is a commonly used method in research studies that aim to find and gather information from instances that are rich and relevant to a given subject of interest or phenomena (Suri, 2011). The use of purposeful sampling in qualitative research serves several important purposes. The researcher is able to gather rich, in-depth data from participants that are most relevant and informative. By selecting participants that are well-suited, and expert to the research field, the researcher can capture the nuances and complexities of the phenomenon within its natural context (Campbell et al., 2020). Furthermore, Purposeful sampling can support the development of theory by enabling the researcher to identify patterns, themes, and insights that may not be accessible through other sampling strategies. In general, it enables the researcher to select participants that can provide the most relevant and information-rich data to address the research objectives (Douglas, 2022).

Qualitative research studies often use a very limited sample size, generally ranging from 12 to 20 people (Sachdeva, 2019). However, the specific number may vary based on factors such as the study methodology, the research question, and the characteristics of the phenomena being investigated. The emphasis is on the comprehensive and detailed nature of the data rather than the statistical adequacy of the sample. Table 3.5 shows the sampling groups contacted and those who responded and agreed to participate.

3.11.3. Participants Selections

Professionals who work as cybersecurity experts, IT managers, executive directors, and IT auditors who have interacted with FinTech innovations were contacted formally to get their agreement to participate in the study. Next, they were approached officially through email with an invitation letter and Participant Information Sheet (PIS). Once they responded with their acceptance to be part of the study, a consent form was shared with them, requesting them to complete the form and send it to the email address. The purpose of the form is to offer a clear explanation of the research subject, its objectives, and the procedures included. The consent form represents an essential value of ethical research practices, especially when it involves humans. This allows potential participants to fully understand the basis of their consent. In addition, the form highlighted possible risks and discomforts related to the research and the participants were notified of their entitlement to withdraw their participation in the research at any time. (See Appendix: 1, 3, and 4).

Table 3.5 Sampling Groups of Participants.

Sampling Groups	Contacted	Agree to participate	Response Rate (%)
Executive Management	5	3	15
Business Owners and Managers	4	4	20
Compliance, Risk, and Law Experts	2	1	5
IT Professionals and Consultants	3	3	15
Cybersecurity Experts	4	2	10
Financial Industry Regulator	2	1	5
Totals	**20**	**14**	**70**

3.12. Data Analysis

Data analysis is among the most crucial tasks in the qualitative research process (Leech & Onwuegbuzie, 2007). The methodologies utilised to analyse qualitative data are determined mainly by the research philosophy and approach. Data analysis is an essential technique that helps researchers in reducing large volumes of data into a meaningful story. According to LeCompte (2000), this technique involves structuring the data, condensing it through summary, and interpreting it through perception. The aim of this process is to make sense of the data and identify patterns or trends that can facilitate the researcher's objective (LeCompte, 2000). The researcher was receptive to new elements revealed inductively via data analysis and was willing to adjust the components of cybersecurity elements appropriately. Pattern matching, which compares an actual pattern to a predicted one, is one of the analytical processes that may be used to analyse qualitative data from a logical viewpoint (Tellis, 1997).

The data collected are analysed using a qualitative data analysis technique that involves coding and thematic analysis of the interview and focus group transcripts.

To analyse qualitative data, there are various general five-point methodologies available that are independent of any particular theoretical perspective. In this research, a typical five-point approach (Figure 3.4) drawn from detailed guidelines (LeCompte, 2000) was adopted.

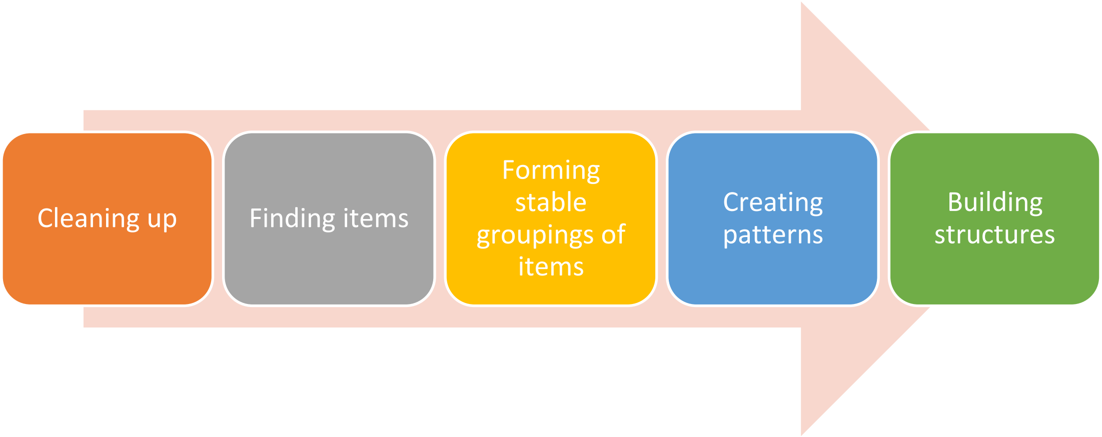


Figure 3.5 Typical five-point approach drawn from LeCompte's (2000)

To analyse qualitative data, LeCompte defined five steps: cleaning up, finding items, forming stable groupings of items, creating patterns, and building structures. These steps are described below:

3.12.1. Cleaning Up

The first step in preparing data for analysis is to clean it up. It allows the researcher to do a brief testing of the data collection. This involves the preparation and revision of the transcribed interview files generated by MS Teams after the end of each virtual interview meeting. They are sorted and named anonymously.

3.12.2. Finding Items

The Nvivo software was used to import the transcribed interviews. Items will emerge through repeated readings of the transcribed interviews to highlight topics relevant to the research questions (or termed as **codes** in Nvivo). NVIVO is used to determine how often the items appeared by displaying their percentages to identify which topics the respondents paid the most attention to.

3.12.3. Forming Stable Groupings of Items

To acquire a comprehensive view of the results, domain analysis (Leech & Onwuegbuzie, 2011) applying semantic correlations (Spradley, 1979) was used for founded items. The researcher makes an effort to combine and contrast the coded topics (items), comparing and contrasting the interviews and the critical risks and cybersecurity control factors to be carried out.

3.12.4. Creating Patterns:

Pattern creation is grouping together concepts that are related to one another in such a manner that they begin to reflect a meaningful explanation or description of the factors under investigation. Defining the most relevant patterns may assist in establishing fundamental principles of the cybersecurity framework for FinTech.

3.12.5. Building Structures:

This stage entails putting together collections of patterns into structures in order to provide a comprehensive description of the proposed cybersecurity framework for FinTech. Composing such a framework may assist stakeholders in better understanding how to address issues, enhance activities, evaluate their efficacy, or build evidence to explain what occurred.

3.13. Results Validation

Since it is exploratory research, the validation exercise of the proposed framework is crucial because it supports the research to ensure that the cybersecurity framework is aligned with financial industry best practices. The validation of qualitative research findings is accomplished via a procedure often referred to as expert review or expert validation. This method should include obtaining input, gaining thoughts, and performing a critical review of the research results from experts who possess knowledge and experience in the specific topic area under research (O. Nyumba et al., 2018). Moreover, the Delphi approach, specifically, has been utilised for conceptual model validation and evaluation. The Delphi approach is appropriate for research involving a new or emerging trend. It has been extensively employed by researchers in policy creation and judgement (Linstone & Turoff, 1975). Numerous uses of the Delphi technique are common in qualitative research. The fundamental idea of this method was to get participants' feedback and arrive at a consensus. To provide more precise and realistic results, Delphi studies could be combined with quantitative data gathering and the use of quantitative techniques to analyse data (Beiderbeck et al., 2021). Findings were validated through experts review and Delphi session.

3.13.1. Experts Review

Expert review plays a crucial role as an external validation process in qualitative research. The use of this approach ensures that the findings are robust, reliable, and trustworthy. By integrating the viewpoints of experts, researchers have the capacity to improve the credibility of their interpretations, augment the applicability of the results, and address any possible biases or constraints that may have been disregarded (Patten, 2016). Primary results summaries were shared with experts. Based on their knowledge, experts critique study results and provide feedback and comments. They evaluated the results' clarity, coherence, and quality in relation to area knowledge, ideas, and concepts (O. Nyumba et al., 2018). Feedback might be remarks, recommendations, or criticisms.

Meeting with experts facilitates the exchange of feedback, clarifies ambiguities, and answers questions and study results. This dialogue improves results validity and collectively establishes a consensus over the interpretation and significance of the results in certain instances. The collaborative nature of this procedure assures that the study results are representative of a shared understanding and consensus among the experts involved (O. Nyumba et al., 2018).

Researchers and professionals may convene to discuss and interpret the results till they reach a consensus (Kelly et al., 2016). This collaborative procedure guarantees that specialists agree on the study results.

3.13.2. Delphi Method

The Delphi method is a technique that involves gathering opinions and conclusions from a panel of experts. The process consists of multiple rounds of surveys, wherein the results are pooled and shared with the group at the end of each round. The experts may change their initial response based on how they perceive the "group response" presented to them in each round. The end result is intended to represent a real consensus on what the group believes (Linstone & Turoff, 1975). The number of cycles in every Delphi process differs, although it rarely exceeds one or two iterations (Rowe & Wright, 1999).

The Delphi approach, specifically, has been utilised for conceptual model validation and evaluation. The Delphi approach is appropriate for research involving a new or emerging trend. It has been extensively employed by researchers in policy creation and judgement (Linstone & Turoff, 1975).

The data may be analysed in various ways, but in the Delphi method, descriptive statistics are often employed to validate the data collected at each round. A technique for analysing changes across Delphi rounds is provided by more complex tools, such as Kendall's W, used in this research. The Delphi method compares and evaluates experts’ responses using descriptive statistics. Responses were quantified using the Likert scale (1-5), and the concordance of feedback and the convergence produced by the Delphi rounds were determined using Kendall's W coefficient. Kendall's coefficient of concordance (W) is a non-parametric statistical measure that quantifies the level of agreement among participants based on rank correlation (Schmidt, 1997).

Thus, for *m* raters rating *n* subjects in rank order from 1 to *n*, and *S* is the squared deviation of rating, the definition of Kendall's W is :

$$W = \frac{12S}{m^2\ (n^3 - n)}$$

Kendall's W is a measure of agreement that ranges from 0 to 1. A score of 0 indicates no agreement, while a score of 1 indicates total agreement, as shown in Table 3.6 (Schmidt, 1997).

Table 3.6 (Schmidt, 1997) Interpretation of Kendall's W coefficient.

W	Interpretation
0	No Agreement
0.10	Weak Agreement
0.30	Moderate Agreement
0.60	Strong Agreement
1	Perfect Agreement

3.14. Ethical Considerations

The ethical principle is associated with the research's professionalism. Since the identified individuals were experts in their areas and work for various private and public sector companies in various roles, they are unable to disclose much sensitive information about actual projects. To eliminate such concerns, each interviewee on the list was given a participant information sheet (PIS) that briefs the research scope and the associated risk, as well as assurances that the interviewee's current post would not be affected. For this reason, the participants were given a consent form in which they agreed to the terms and conditions, which included consenting to participate voluntarily and having the right to be informed about the research's content and findings at any time, along with a statement from the researcher stating that there are no particular advantages to participating and that there are no risks to the participant. The participants were also told that the interview discussion would be recorded for transcription purposes and then deleted after the study was completed. Furthermore, although the data that was gathered was centred on gathering some essential generic characteristics information, no identifiable information about the participants were acquired. No particular personal information, such as name, email, phone number, or workplace, were disclosed at any part of the study. The results of this research would help both public and private sector companies and will advance knowledge in the development of cybersecurity framework, along with common cybersecurity resources to support FinTech by protecting them from cyber risks.

Ensuring diversity and inclusivity in research is crucial for obtaining reliable, representative, and unbiased findings. Gender balance is considered, and it is essential in research to guarantee representative and unbiased findings. This is achieved by equal representation of genders within research samples. It is also expected to be aware of their own potential gender biases and to take steps to mitigate them throughout the research process. Disaggregating data by gender and using gender-neutral language in research materials are additional strategies that were employed to ensure gender balance in research. Moreover, the inclusion of people with various levels of experience is considered. This would guarantee that the study included a diverse array of perspectives. The contributions of specialists and experts with relevant expertise in the investigated topic are very significant. This point is considered while recruiting participants with varying levels of experience. Another consideration is to include different types of management groups in the study, and it is deemed important to ensure that research methods and materials are culturally sensitive to all these levels.

3.15. Research Challenges

The researcher is constrained to a few current cybersecurity research papers and publications, particularly those related to Bahrain's financial organisations. Secondary data are primarily based on existing frameworks and standards from other international bodies in the United States and Europe, where the cybersecurity factors and priorities may differ from those in the region or Bahrain. Furthermore, considering cybersecurity is a sensitive topic of discussion, some research participants might be unwilling to disclose significant security information related to their businesses. This was addressed using (PIS), by assuring participant's information will stay protected and safely handled. Another limitation of this research is the fact that setting up interview meetings with most business experts from different cybersecurity stakeholders is challenging to arrange promptly. As a mitigating approach, the researcher created two options for meeting times, preferably outside of their busy business hours.

3.16. Summary

This chapter outlined the research approach for investigating cybersecurity in FinTech through the lens of Socio-Technical Systems (STS). It detailed how technology, people, processes, and environmental factors will be operationalised and measured.

By adopting a pragmatic research philosophy and employing a combination of deductive and inductive reasoning, this research aims to develop a comprehensive and tailored cybersecurity framework for FinTech innovations in Bahrain. The study utilised exploratory and conclusive research designs, collected qualitative data, and analysed the data using appropriate techniques. In this chapter, the research gap and qualitative methodology were discussed. The research strategy and research instrument design were explained based on the identified research questions and objectives.

Primary data were collected through semi-structured interview questions from financial institute employees, executives, and FinTech experts in Bahrain. The use of qualitative research techniques resulted in a deeper understanding of the framework’s key principles and fulfilled the research’s objectives.

Section 3.5 explained the framework development methodology and how the STS framework will guide the selection of participants, the formulation of interview questions, and the interpretation of the findings.

The researcher formulated study goals, enquiries, and a qualitative data-gathering method to fully comprehend cybersecurity in Bahrain's FinTech industry. Expert insights were captured through in-depth interviews with cybersecurity professionals, IT managers, and executive directors from key Bahraini FinTech businesses.

The qualitative data gathered was analysed using theme analysis to identify recurring patterns and extract significant results. In order to strengthen the study's precision, focus groups and Delphi rounds were employed to validate and refine these results, eventually guiding the establishment of a cybersecurity framework for the Bahraini FinTech field.

Before collecting data, ethical permission was obtained from the relevant review panel (see Appendix 5 Ethics Approval). After obtaining ethical approval, we conducted primary data collection and analysis to interpret the research findings and drive the development of the cybersecurity framework.

Chapter 4: Data Collection and Findings

4. Chapter 4: Data Collection and Findings

4.1. General Overview

The data collection for this study is conducted using semi-structured interviews as described in Chapter 3, enabling the researcher to analyse the findings within a structured context of the financial sector in Bahrain.

The data was collected from 14 interviews that were conducted, interpreted, and presented using thematic analysis. The sample selected from recruited participants of user interviews is described in this chapter, along with the participants' related characteristics and how their privacy is protected throughout this qualitative research. This chapter will exhibit an analysis of the empirical results obtained from the performed interviews. These findings will then be synthesised in relation to the literature review presented in Chapter 2, leading to the development of a cybersecurity framework for FinTech in Bahrain.

This chapter comprehensively describes the sample used in the study and thoroughly explains how the collected data is gathered. It highlights the identified FinTech stakeholders in Bahrain, providing insights into the key players and entities in the FinTech industry within the research context. Then, it outlines the qualitative data analysis approach used to analyse the collected data. Furthermore, it provides an overview of the framework development process, including the methodology used and the key factors considered. Finally, it presents a detailed exploration of the recommended principles and controls within the proposed cybersecurity framework, enhancing the understanding of the research findings and their implications for addressing cybersecurity concerns in the FinTech sector.

4.2. Description of the Sample

The sample consisted of 14 participants who worked at Bahrain’s financial institutions and had expertise in the FinTech and cybersecurity field. Table 4.1 describes the posts of the research sample.

The 14 participants were assigned to one of three groups: Operational and entry-level or similar, Middle management or comparable, and Senior management or equivalent post as shown in the second column of Table 4.2.

Table 4.1 Posts of the Research Sample

Board and executive management
IT Managers and Business Owners
Risk, compliance, and legal specialists
IT auditors and consultants
Cybersecurity Experts
Financial industry Regulator

4.2.1. General Characteristics

Table 4.2 uses alphanumeric identifiers (P*x*) instead of names to illustrate the characteristics of the 14 research participants. The characteristics information includes the participant's management level (Column 2), number of experience years in the field (Column 4), the firm's line of business (Column 5), and number of employees in the financial institution (Column 6). It should be noted that the number of years of experience shapes perspectives, knowledge, and attitudes, which are central to qualitative inquiry and could significantly influence the results. Experienced participants can provide in-depth insights, nuanced perspectives, and detailed narratives due to their extensive exposure to the phenomenon under study. Participants can offer valuable technical context, enabling the researcher to understand how the phenomenon has evolved over time. Their experience might equip them with critical thinking skills to articulate complex issues and provide thoughtful feedback. In addition, their insights can be used to validate or challenge emerging patterns and themes in the data. However, long-term experiences might be influenced by hindsight bias, and participants might feel pressure to provide socially acceptable answers rather than honest opinions. Moreover, extensive experience could lead to overconfidence in their opinions, limiting the exploration of alternative viewpoints.

Table 4.2 Participants' characteristics information

Identifier	**Management Level**	**Qualification**	**Experience years**	**Business line**	**No of Employees**	**Duration (Min)**
P1	Middle management	BSc in Computer Science	12	Regulator	400	69.00
P2	Senior management	MBA	20	FinTech	130	56.00
P3	Middle management	MSc Security and Informatics	15	Bank	400	33.00
P4	Senior management	MBA	20	FinTech	15	65.00
P5	Operational	MBA	18	Bank	350	43.00
P6	Middle management	MBA	25	Bank	97	50.00
P7	Middle management	BSc Business Information System	20	Bank	350	43.00
P8	Middle management	BSc Computer Engineering	14	Bank	80	96.00
P9	Senior management	MSc in Computer Science	30	FinTech	130	45.00
P10	Operational	MSc Information Security	24	Consultancy	300	57.00
P11	Operational	MBA	15	Bank	750	48.00
P12	Middle management	MBA	14	FinTech	500	51.00
P13	Middle management	PhD	9	Bank	70	44.00
P14	Senior management	MSc in Computer Science	28	FinTech	72	63.00

4.2.2. Data Collection Method

During COVID-19 and due to the pandemic retractions, all interviews were conducted virtually using **MS Teams** 365 audioconferencing software, and the data was collected between January and April 2023. The 14 interviews lasted 763 minutes in total. Each interview lasted an average of 54 minutes. In Table 4.2, the most extended session was 96 minutes long, while the shortest was just 33 minutes long.

4.2.3. Interviews Records

The participant's answers were recorded (with consent) and transcribed to text files using MS Teams. The researcher first accessed the MS Teams meeting transcript by opening the meeting in the chat and clicking the three dots (...) next to the recording. The transcript is then downloaded as a DOCX file.

Before the text file was prepared for import, some tidying up was needed. The downloaded DOCX file was opened in a text editor like Notepad. As MS Teams transcripted separate participants turns with dashes (-), these dashes were replaced with paragraph breaks using the "Find and Replace" function. The specific replacement character, "^p^p" (two carriage returns) or "^p" (single carriage return), depended on the researchers' preference for spacing between participants. Finally, the edited transcript was saved as a plain text file (.txt).

Upon preparing the text file, the "Import" function was selected in the NVivo software, followed by "Text Files" from the available options. The prepared text file was then chosen, and the appropriate import options were set. This process is repeated for all interviews to be successfully imported into NVivo 12.0, making them ready for analysis.

4.2.4. Coding and Analysis Using Nvivo

After that, many rounds of analysis were carried out. Each transcript was first-hand-coded and constituted a dataset inside the corresponding interview discussion. To guarantee that the analyses, themes, and supporting patterns were aligned with the research question, the first set of codes was obtained from the research questions. As a result, the first codes were created to deal with semi-structured interview content. These early codes also included a set of sub-codes to keep track of which interview question was answered. For further categorisation and thematic analysis, the manually coded datasets were saved into the NVivo software.

Another level of analysis using the NVivo software was performed, including pattern coding and classification. In order to fulfil the requirement of theme analysis, this extra analysis required looking for repeated patterns in all of the data connected to the research questions. The thematic analysis comprises the recursive investigation and evaluation of codes, themes, and patterns in order to establish their validity in relation to the data obtained (Clarke & Braun, 2017). This increased consistency provides an assurance of quality and is an advantage of using the theme analysis technique.

4.2.5. Participants' Privacy and Confidentiality

Before taking part in this study, each participant signed an informed consent form in order to be fully informed about the research and all privacy and confidentiality precautions. In this study, participants are simply identified using an alphanumeric coded identification (Px) rather than personally identifying details. None of the participants' personally identifiable information was kept. During the data collection and analysis phases, participants were entirely anonymous, and their names were never connected with interview codes. The data from the participants and the notes will be destroyed after ten years, and any digital recordings will be deleted completely.

4.2.6. Identified FinTech Stakeholders in Bahrain.

During interviews and discussions with the experts, FinTech services vary from traditional financial services in a number of fundamental ways. First was the customer domain, in which services were provided to customers in an innovative model, mainly through smart devices. The other point is the transaction medium, which is technologically intensive, comprising self-service financial activities completed through a smart device using data service over telecom networks.

An abstracted service model for FinTech stakeholders in Bahrain was drawn to serve as both a reference and a classifying scheme. The service model used in the investigation of cybersecurity threats for FinTech is shown in Figure 4.1. The diagram depicted the wide variety of players engaged in the delivery of FinTech services, as well as the many ways in which they are connected and interacted. Moreover, it would facilitate the comprehension of the relationships between customers, entities, agents, layers, and functions in Bahrain's financial sector. The service model established a shared understanding of a FinTech ecosystem and the cyber threats and risks surrounding it.

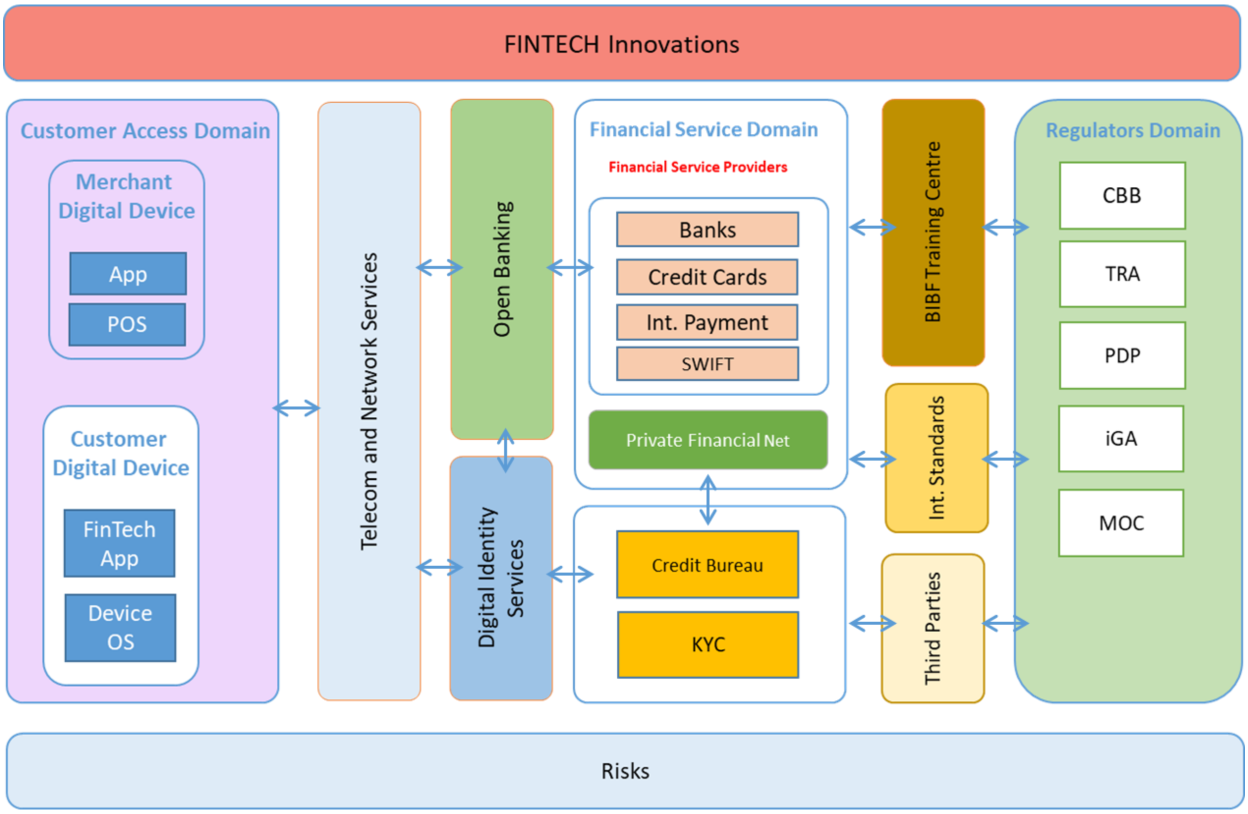


Figure 4.1 The service Model of the Identified FinTech stakeholders in Bahrain.

Because of the several threat possibilities and the lack of available defences, the cybersecurity challenges that such services confront are slightly diverse. Aside from the risks immediately addressed by cybersecurity frameworks deployed and effectively used in the financial institutes in Bahrain, there are very specific types of risk that such frameworks do not manage, given the environment in which they were designed. In general, these frameworks do not consider national laws and regulation enforcement as illustrated in the regulation domain in Figure 4.6.

4.3. Data Coding Using the Theoretical Framework

As discussed in Chapter 2, FinTech can be viewed as a socio-technical system STS that comprises two dimensions, social and technical, all acting within a wider environment, as shown in Figure 2.6. In the context of cybersecurity, a socio-technical system may be defined as a designed arrangement including people and users, with a focus on security. This arrangement interacts with many subsystems while taking security concerns into consideration.

1. A technological security subsystem that aims to achieve and sustain a customised security arrangement. Staff and users utilise security-specific knowledge, skills, techniques, tools, equipment, and facilities to achieve and maintain specific security

goals. They are collaborating on coordinated operations and procedures to achieve the specified security targets.

2. A social security subsystem is established to provide a customised security arrangement for staff and users in social connections. The coordinating setup ensures that the operations of the organisation are effectively planned and controlled to achieve the objectives of system security.

Each individual subsystem element and characteristic has the potential to impact the overall security of the system since they all interact and contribute to the system's regular operation and security (Ani et al., 2023).

Therefore, the cybersecurity framework may be characterised as a comprehensive arrangement that utilises a combination of technological, structural, social, and administrative traits and capabilities to achieve specific cybersecurity objectives.

The initial set of codes was created based on the STS model to guarantee consistency between the STS theoretical framework's analysis, themes, and supporting patterns with the research question. Thus, the initial codes were created to tackle the content of semi-structured interviews pertaining to social and technical dimensions. The early codes included a series of Structure, Actors, Technology, and Work activities sub-codes to monitor which interview question was addressed when the coded quote was made.

4.4. Qualitative Data Analysis Approach

Data analysis is among the most crucial tasks in the qualitative research process (Leech & Onwuegbuzie, 2007). As discussed in Chapter 3, section 3.12, LeCompte (2000) mentioned that throughout the analysis, three things happen: data is structured, data is condensed via summary and classification, and patterns and themes in the data are recognised and connected (LeCompte, 2000). Therefore, it is easier to discover the factors influencing FinTech's cybersecurity controls by utilizing the existing literature and LeCompte's methodology. It's possible that these theoretical assumptions diverge significantly from what the participants think.

4.4.1. Themes and Supporting Patterns

As discussed in Chapter 3, to analyse qualitative data, there are various general five-point methodologies available that are independent of any particular theoretical perspective. In this research, a typical five-point approach (Figure 3.5) drawn from detailed guidelines (LeCompte, 2000) was adopted. To analyse qualitative data, LeCompte defined five steps: cleaning up, finding items, forming stable groupings of items, creating patterns, and building structures. These are described below, along with the techniques that should be used in the sub-processes.

Using the above qualitative analysis methodology, this section presents the common themes and their supporting patterns throughout the data collected by interviewing the sample groups. It focuses further on the research themes resulting from collected data and describes the critical aspects involved in developing a cybersecurity framework for FinTech stakeholders in Bahrain.

4.4.1.1. Cleaning Up

The first step in preparing data for analysis is to clean it up. It allows the researcher to do a brief testing of the data collection. This involves the preparation and revision of the transcribed interview files generated by MS teams after the end of each virtual interview meeting. They are sorted and named anonymously.

4.4.1.2. Finding Items

Nvivo was utilised to import the transcribed interviews. Items will emerge through repeated readings of the transcribed interviews to highlight topics related to the research questions (or called as codes in Nvivo).

Table 4.3 lists 36 items that resulted from the analysis of the 14 individuals' interview sessions.

Table 4.3 Items emerged from Interviews.

Items	**No of Ref.**	**P1**	**P10**	**P11**	**P12**	**P13**	**P14**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1: Capacity Building and Awareness	**11**	0	0	1	0	1	2	0	1	0	2	0	0	3	1
2: Awareness Activities	**47**	1	2	3	6	4	6	3	3	3	1	3	3	5	4
3: Customer Protection	**15**	0	1	0	3	3	2	0	0	0	0	0	2	2	2
4: Human Resources	**27**	1	6	2	3	1	2	2	0	0	2	3	1	1	3
5: IT Staff training	**32**	3	1	5	5	2	1	4	1	0	2	4	3	1	0
6: Knowledge Mgt & Capacity	**22**	1	3	1	1	2	1	0	1	3	1	4	2	1	1
7: Regulation and Governance	**15**	7	1	0	0	0	1	0	0	1	0	0	3	0	2

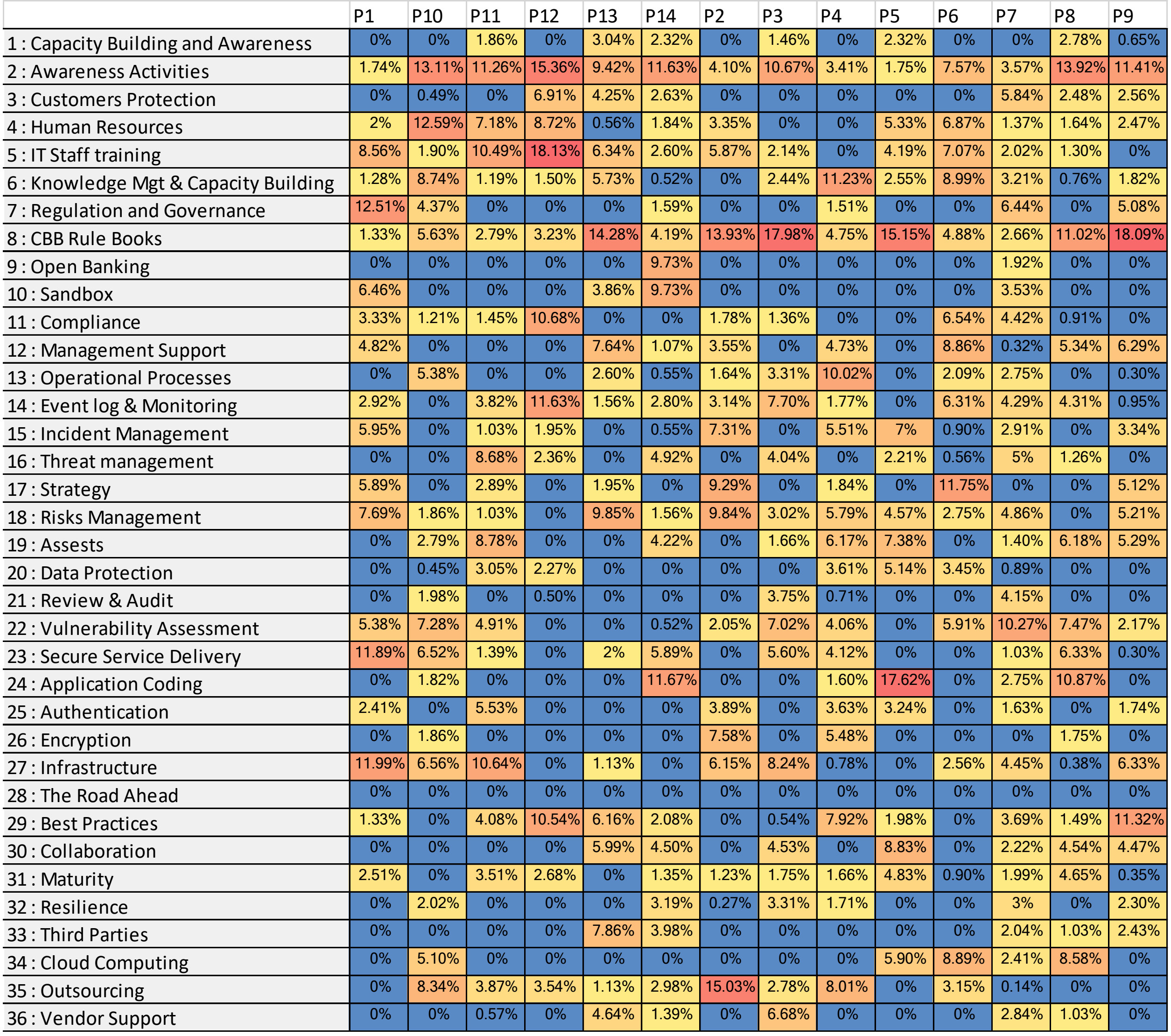
8: CBB Rule Books	**38**	1	3	3	1	3	1	3	5	3	4	1	2	4	4
9: Open Banking	**2**	0	0	0	0	0	1	0	0	0	0	0	1	0	0
10: Sandbox	**7**	2	0	0	0	1	1	0	0	0	0	0	3	0	0
11: Compliance	**17**	1	1	2	4	0	0	2	1	0	0	3	2	1	0
12: Management Support	**17**	1	0	0	0	3	1	2	0	2	0	2	1	3	2
13: Operational Processes	**13**	0	1	0	0	2	1	1	1	4	0	1	1	0	1
14: Event log & Monitoring	**26**	1	0	3	4	1	2	3	3	1	0	2	3	2	1
15: Incident Management	**14**	1	0	2	1	0	1	2	0	2	1	2	1	0	1
16: Threat management	**13**	0	0	4	1	0	1	0	1	0	1	1	3	1	0
17: Strategy	**11**	1	0	3	0	2	0	2	0	1	0	1	0	0	1
18: Risks Management	**21**	2	1	1	0	3	1	3	2	3	1	1	2	0	1
19: Assets	**19**	0	1	3	0	0	3	0	1	3	2	0	2	3	1
20: Data Protection	**11**	0	1	1	1	0	0	0	0	3	1	3	1	0	0
21: Review & Audit	**7**	0	1	0	1	0	0	0	2	1	0	0	2	0	0
22: Vulnerability Assessment	**27**	1	5	4	0	0	1	2	3	2	0	2	4	2	1
23: Secure Service Delivery	**14**	3	2	1	0	1	2	0	1	1	0	0	1	1	1
24: Application Coding	**17**	0	2	0	0	0	2	0	0	1	6	0	2	4	0
25: Authentication	**16**	1	0	3	0	0	0	3	0	3	2	0	3	0	1
26: Encryption	**6**	0	1	0	0	0	0	3	0	1	0	0	0	1	0
27: Infrastructure	**23**	2	2	4	0	1	0	4	3	1	0	1	1	1	3
28: The Road Ahead	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29: Best Practices	**23**	1	0	2	3	3	1	0	1	2	1	0	4	2	3
30: Collaboration	**14**	0	0	0	0	2	2	0	2	0	4	0	2	1	1
31: Maturity	**13**	1	0	1	1	0	1	1	1	1	2	1	1	1	1
32: Resilience	**10**	0	1	0	0	0	2	1	1	1	0	0	3	0	1
33: Third Parties	**9**	0	0	0	0	2	3	0	0	0	0	0	1	1	2
34: Cloud Computing	**13**	0	3	0	0	0	0	0	0	0	2	3	3	2	0
35: Outsourcing	**14**	0	2	2	1	1	1	1	1	2	0	2	1	0	0
36: Vendor Support	**8**	0	0	1	0	1	1	0	2	0	0	0	2	1	0

Table 4.3 demonstrates that all of the items included in the factors relevant to the cybersecurity and FinTech were agreed upon by all of the participants. The researcher assumes that the frequency of words and themes offers a decent indicator of meaningfulness, as (Leech & Onwuegbuzie, 2007) found word count beneficial. In this case, word count was utilised to

determine and analyse the participants’ attention to the Figures (4.2 and 4.3). The word count in terms of '% coverage' (Table 4.4), which represents the number of characters as a proportion of the overall source, was generated using NVivo's constant comparison analysis tool.

Word clouds are useful for visually representing qualitative data because they are easy to use and give fast insights into a look-through depiction of word frequency. The bigger the word appears in the graphic created, the more often the keyword occurs in the text being analysed. Word clouds are becoming more common as an easy approach to identify the focus of written material.

Table 4.4 The word count in terms of '% coverage'



	P1	P10	P11	P12	P13	P14	P2	P3	P4	P5	P6	P7	P8	P9
1 : Capacity Building and Awareness	0%	0%	1.86%	0%	3.04%	2.32%	0%	1.46%	0%	2.32%	0%	0%	2.78%	0.65%
2 : Awareness Activities	1.74%	13.11%	11.26%	15.36%	9.42%	11.63%	4.10%	10.67%	3.41%	1.75%	7.57%	3.57%	13.92%	11.41%
3 : Customers Protection	0%	0.49%	0%	6.91%	4.25%	2.63%	0%	0%	0%	0%	0%	5.84%	2.48%	2.56%
4 : Human Resources	2%	12.59%	7.18%	8.72%	0.56%	1.84%	3.35%	0%	0%	5.33%	6.87%	1.37%	1.64%	2.47%
5 : IT Staff training	8.56%	1.90%	10.49%	18.13%	6.34%	2.60%	5.87%	2.14%	0%	4.19%	7.07%	2.02%	1.30%	0%
6 : Knowledge Mgt & Capacity Building	1.28%	8.74%	1.19%	1.50%	5.73%	0.52%	0%	2.44%	11.23%	2.55%	8.99%	3.21%	0.76%	1.82%
7 : Regulation and Governance	12.51%	4.37%	0%	0%	0%	1.59%	0%	0%	1.51%	0%	0%	6.44%	0%	5.08%
8 : CBB Rule Books	1.33%	5.63%	2.79%	3.23%	14.28%	4.19%	13.93%	17.98%	4.75%	15.15%	4.88%	2.66%	11.02%	18.09%
9 : Open Banking	0%	0%	0%	0%	0%	9.73%	0%	0%	0%	0%	0%	1.92%	0%	0%
10 : Sandbox	6.46%	0%	0%	0%	3.86%	9.73%	0%	0%	0%	0%	0%	3.53%	0%	0%
11 : Compliance	3.33%	1.21%	1.45%	10.68%	0%	0%	1.78%	1.36%	0%	0%	6.54%	4.42%	0.91%	0%
12 : Management Support	4.82%	0%	0%	0%	7.64%	1.07%	3.55%	0%	4.73%	0%	8.86%	0.32%	5.34%	6.29%
13 : Operational Processes	0%	5.38%	0%	0%	2.60%	0.55%	1.64%	3.31%	10.02%	0%	2.09%	2.75%	0%	0.30%
14 : Event log & Monitoring	2.92%	0%	3.82%	11.63%	1.56%	2.80%	3.14%	7.70%	1.77%	0%	6.31%	4.29%	4.31%	0.95%
15 : Incident Management	5.95%	0%	1.03%	1.95%	0%	0.55%	7.31%	0%	5.51%	7%	0.90%	2.91%	0%	3.34%
16 : Threat management	0%	0%	8.68%	2.36%	0%	4.92%	0%	4.04%	0%	2.21%	0.56%	5%	1.26%	0%
17 : Strategy	5.89%	0%	2.89%	0%	1.95%	0%	9.29%	0%	1.84%	0%	11.75%	0%	0%	5.12%
18 : Risks Management	7.69%	1.86%	1.03%	0%	9.85%	1.56%	9.84%	3.02%	5.79%	4.57%	2.75%	4.86%	0%	5.21%
19 : Assests	0%	2.79%	8.78%	0%	0%	4.22%	0%	1.66%	6.17%	7.38%	0%	1.40%	6.18%	5.29%
20 : Data Protection	0%	0.45%	3.05%	2.27%	0%	0%	0%	0%	3.61%	5.14%	3.45%	0.89%	0%	0%
21 : Review & Audit	0%	1.98%	0%	0.50%	0%	0%	0%	3.75%	0.71%	0%	0%	4.15%	0%	0%
22 : Vulnerability Assessment	5.38%	7.28%	4.91%	0%	0%	0.52%	2.05%	7.02%	4.06%	0%	5.91%	10.27%	7.47%	2.17%
23 : Secure Service Delivery	11.89%	6.52%	1.39%	0%	2%	5.89%	0%	5.60%	4.12%	0%	0%	1.03%	6.33%	0.30%
24 : Application Coding	0%	1.82%	0%	0%	0%	11.67%	0%	0%	1.60%	17.62%	0%	2.75%	10.87%	0%
25 : Authentication	2.41%	0%	5.53%	0%	0%	0%	3.89%	0%	3.63%	3.24%	0%	1.63%	0%	1.74%
26 : Encryption	0%	1.86%	0%	0%	0%	0%	7.58%	0%	5.48%	0%	0%	0%	1.75%	0%
27 : Infrastructure	11.99%	6.56%	10.64%	0%	1.13%	0%	6.15%	8.24%	0.78%	0%	2.56%	4.45%	0.38%	6.33%
28 : The Road Ahead	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
29 : Best Practices	1.33%	0%	4.08%	10.54%	6.16%	2.08%	0%	0.54%	7.92%	1.98%	0%	3.69%	1.49%	11.32%
30 : Collaboration	0%	0%	0%	0%	5.99%	4.50%	0%	4.53%	0%	8.83%	0%	2.22%	4.54%	4.47%
31 : Maturity	2.51%	0%	3.51%	2.68%	0%	1.35%	1.23%	1.75%	1.66%	4.83%	0.90%	1.99%	4.65%	0.35%
32 : Resilience	0%	2.02%	0%	0%	0%	3.19%	0.27%	3.31%	1.71%	0%	0%	3%	0%	2.30%
33 : Third Parties	0%	0%	0%	0%	7.86%	3.98%	0%	0%	0%	0%	0%	2.04%	1.03%	2.43%
34 : Cloud Computing	0%	5.10%	0%	0%	0%	0%	0%	0%	0%	5.90%	8.89%	2.41%	8.58%	0%
35 : Outsourcing	0%	8.34%	3.87%	3.54%	1.13%	2.98%	15.03%	2.78%	8.01%	0%	3.15%	0.14%	0%	0%
36 : Vendor Support	0%	0%	0.57%	0%	4.64%	1.39%	0%	6.68%	0%	0%	0%	2.84%	1.03%	0%

Figure 4.3 highlighted keywords like Cyber, Security, People, Organisation, Information, Controls, Risk, Process, etc, as more frequent topics and areas during the interviews. Incorporating concepts from the STS theoretical framework discussed in the literature shows how people, processes, and technology interact in reference to the cybersecurity model for FinTech.

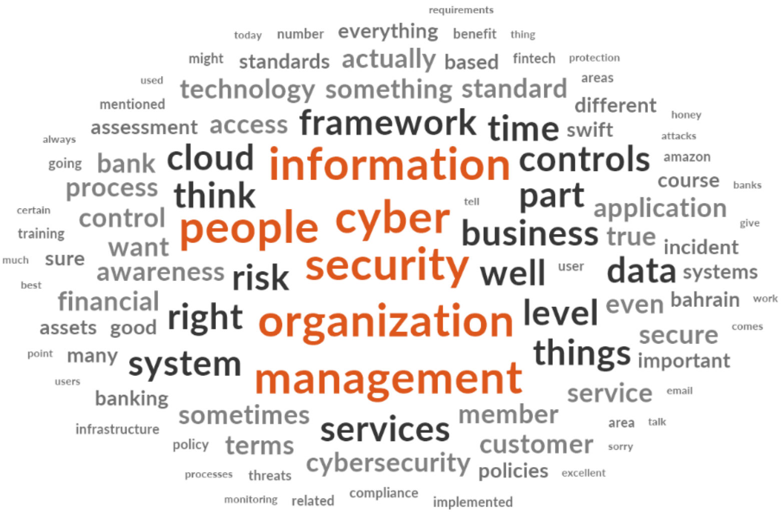


Figure 4.2 Codes Word Cloud

Out of Nvivo software, these are the coded factors that participants emphasised during their interviews. These are mapped using the STS theoretical framework as shown in Table 4.5

Table 4.5 Social and Technical Dimensions Attributes.

Social dimension		**Technical dimension**	
Structure	Attributes	**Technology**	Attributes
How the organization is arranged including both formal and informal authority structures	• Management Support • Open Banking • Sandboxing • Compliance • Outsourcing • Vendor Profile & Support	Tools and technology resources employed by the organization.	• Application Coding • Authentication • Assets Management • Encryption • Secure Infrastructure • Cloud Computing • Future Scalability
Actors	Attributes	**Work Activities**	Attributes

The behaviour of people, individuals and teams in the organization.	• Awareness Activities • Communications • IT Staff skills training • Knowledge Mgt & Capacity Building • Maturity • Collaboration	Tasks, processes and procedures used in relation to technology.	• CS Strategy & Policy • Operational Processes • Review & Audit • Vulnerability Assessment • Risk Mitigation • CBB CS Rule Books • Resilience

For instance, interviewees emphasised the significance of Capacity Building and Awareness Regulation and Governance (Figure 4.3) as essential topics to address cybersecurity controls for FinTech in Bahrain.

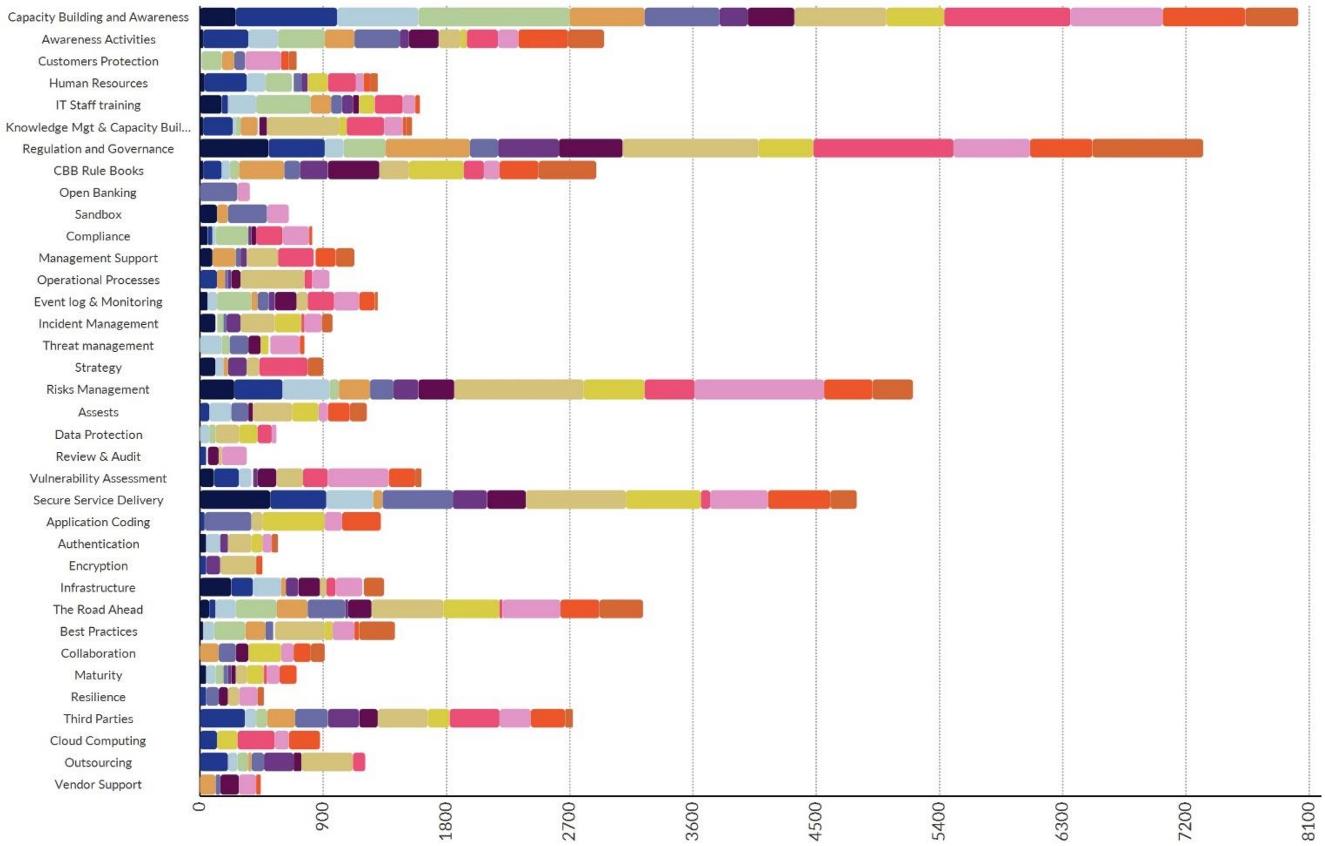


Figure 4.3 Matrix Coding and word count.

Based on the thoughts the participant expressed, themes were developed. NVivo was used to determine how often the items appeared by displaying their percentages (Table 4.4) to identify which topics the respondents paid the most attention to.

4.4.1.3. Forming Stable Groupings of Items

To fully comprehend the results, the researchers used domain analysis (Leech & Onwuegbuzie, 2011) employing semantic correlations (Spradley, 1979) on the 36 items. After the identification of initial elements, it is required to categorise them by means of comparing and contrasting or combining and arranging them. The objective of this exercise is to facilitate the grouping of elements that exhibit similarity or have a logical connection. Researchers seek to identify similarities, subtle variations requiring adjustments to original descriptions, significant differences, or contradictory elements in order to establish separate categorisations for various objects (LeCompte, 2000). The researcher looks for any additional groupings that may result from the opinions of the participants. Some of them produced distinctive insights and created a valid group of items.

4.4.1.4. Creating Patterns:

Pattern generation involves the organisation of interconnected ideas in a way that forms a coherent and understandable explanation or description of the aspects being studied. Identifying the most significant trends may help develop core elements of the cybersecurity framework for FinTech. By analysing the semantic relationships (Parfitt, 1996) between different items, researchers can gain insights into how to categorise, understand, and relate concepts within a specific cultural context.

The relationships between several emerging themes related to the people factor are shown in Figure 4.4. For example, it shows that cybersecurity awareness activities are part of **Capacity Building and Awareness's** main theme.

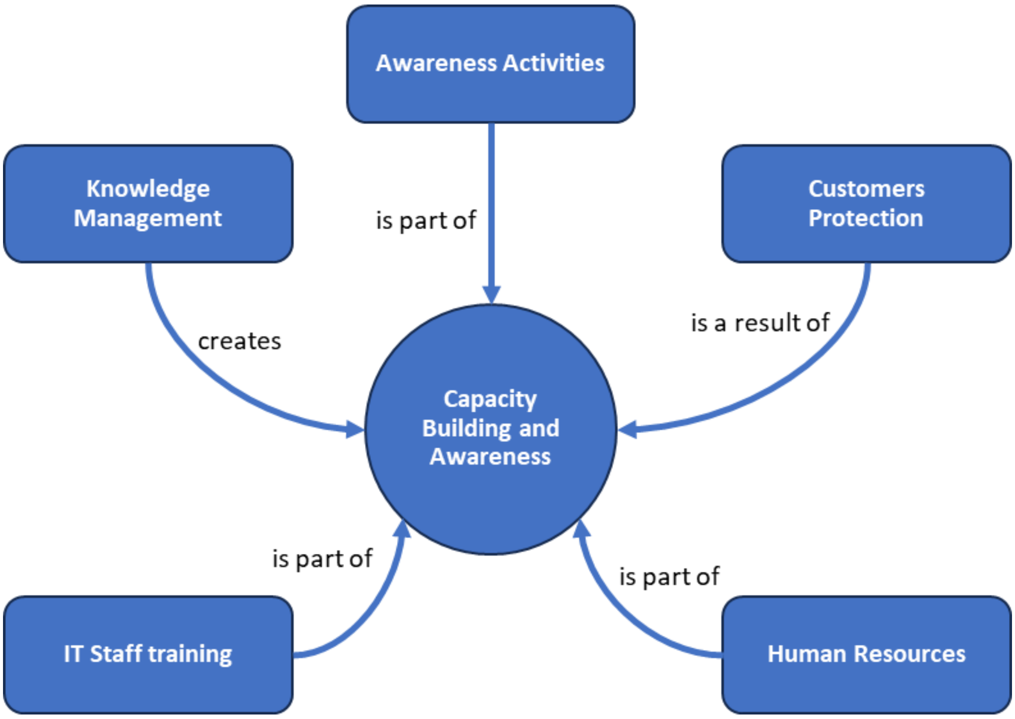


Figure 4.4 The relationship of Capacity Building and Awareness and other factors.

All respondents mentioned the significance of staff awareness training and its frequency to leverage the level of cybersecurity awareness and capacity building. P3 mentioned, “You can have all of the technology in the world. It won't do anything if, the human factor fails.” At the same time, P4 states that “we do cybersecurity awareness programs in a much easier way, which is online. Staff are taking the material out there with self-learning study, then they attend an online exam and will receive a completion certificate if they finished.” However, P5 adopted a simulation scenario for phasing emails and tested the users’ behaviour in responding to these fake emails with the correct link to short online sessions for specific cybersecurity awareness topics. Knowledge management creates a higher level of capacity building and awareness for a financial institute, as per the P14 responded.

While discussing cybersecurity **Regulation and Governance**, most of the respondents emphasized the importance of following the CBB rulebooks as it contains mandated guidelines and control from the main financial regulator in Bahrain (Figure 4.5). FinTech has to go through the sandbox check to validate its compliance with all rules and regulations.

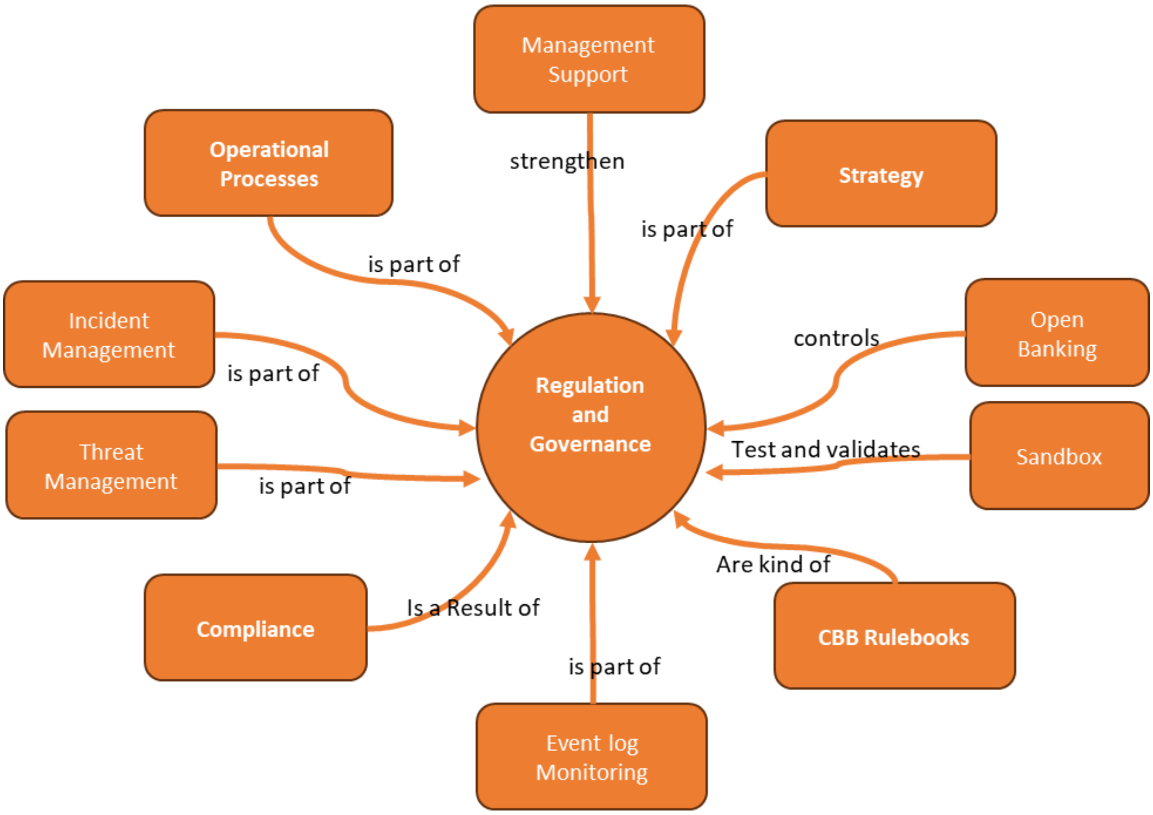


Figure 4.5 The relationship of Regulation and governance and other factors.

P7 detailed that any FinTech innovation to start a business in Bahrain should go through a rigorous check using the regulatory sandbox provided by CBB. It will not be licenced unless it confirms its readiness and compliance with cybersecurity predefined checks, such as penetration test procedures, business continuity plans, and other security operational processes. In other words, this verifies and makes it easier to onboarding new FinTech players with his business.

CBB is insisting on compliance within its rulebooks, and it's mandated that, even if you are adopting another international standard like PCI DSS for card payments, P5 reported. P1, P2, P11, and P13 highlighted that Confidentiality, Availability and Integrity of the data are part of the cybersecurity strategy for any organisation. This strategy is supported by the top management, and every employee should be aware of it.

Twelve participants consider that **Risk Management** includes areas like asset protection, data protection, and vulnerability assessment (Figure 4.6). P8 contributes: “In order to be proactive, we do a monthly phishing simulation for our employees just to assess and measure the awareness in terms of security. Let's say we can call it a human vulnerability assessment.” P4, P7, and P10 talked about customer data protection, and data is the first of all to be secured. They are uncertain if FinTech implements a Personal Data Protection Law (PDPL) or if they are treating customers’ data seriously as per the privacy law here in Bahrain. All participants agree that all staff involvement with the FinTech platform must be tracked, and those records must be authoritative.

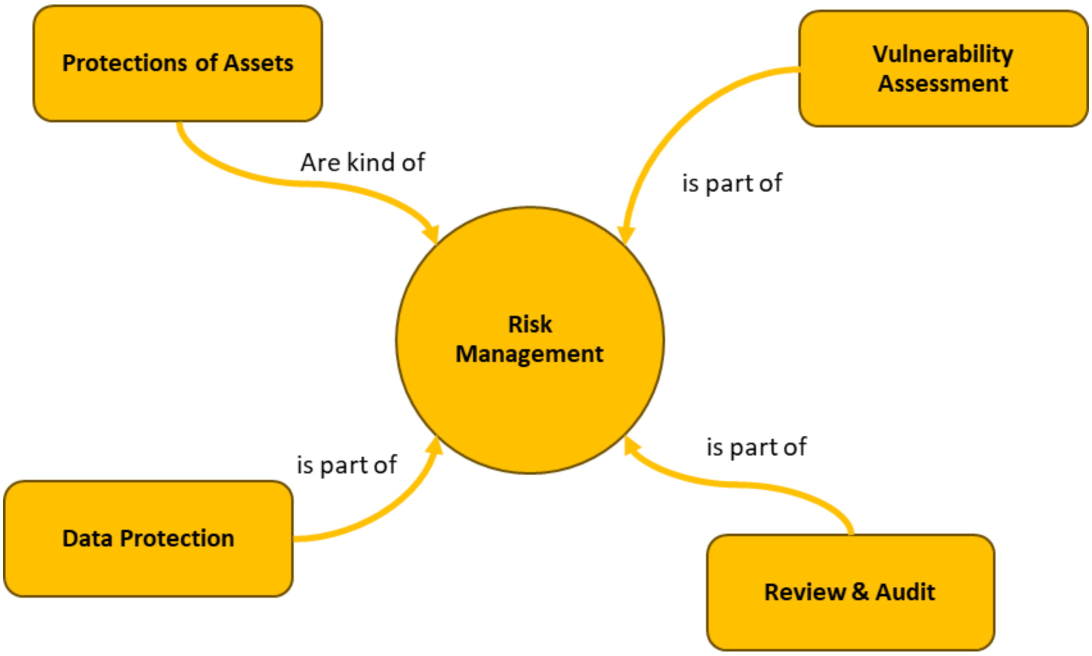


Figure 4.6 The relationship of Risk Management and other factors.

Figure 4.7 shows the relationship between **Secure Delivery of Service** and the factors that fall under its domain.

All interviewees emphasised that FinTech businesses should take high measures to guarantee that end-to-end security exists between their internal systems and customers' systems. Other exterior systems and networks should not be trusted for security. P1 points out that users should be forced to verify themselves using a tool whenever they initiate a transaction or access confidential data. Multi-factor authentication (MFA), including biometrics, should be considered.

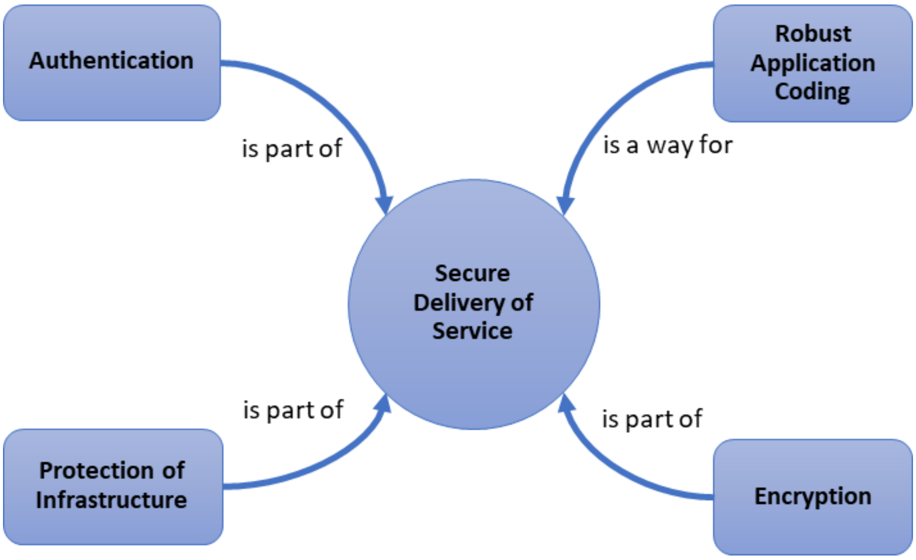

Authentication
is part of
Robust Application Coding
is a way for
Secure Delivery of Service
is part of
Protection of Infrastructure
is part of
Encryption

Figure 4.7 The relationship of Secure Delivery of Service and other factors.

Moreover, P2, P4, P8, and P10 insisted that encryption is essential for FinTech functioning as well as data security and privacy. It contributes to the integrity and confidentiality of data in transmission. All data, both in transit and at rest, must be encrypted. The FinTech mobile application's designers should embed code protections against cyber-attacks. Furthermore, the application should be encrypted so that an intruder cannot retrieve data and keys, as reported by P1, P4, P5, P8, and P10. On the other side, P2, P3, and P4 highlighted that FinTech firms should secure their core infrastructure, such as digital identity mechanisms, payment gateways, and financial exchanges.

The majority of participants encourage FinTech to embrace and execute recognised cybersecurity standards. When implemented correctly, this will facilitate compliance and resilience with ongoing regulatory needs easier. To improve the cybersecurity of their systems, the FinTech IT department should implement and execute worldwide **Best Practices** cybersecurity systems. They should acquire the capacity to detect and respond to new cybersecurity threats as they arise.

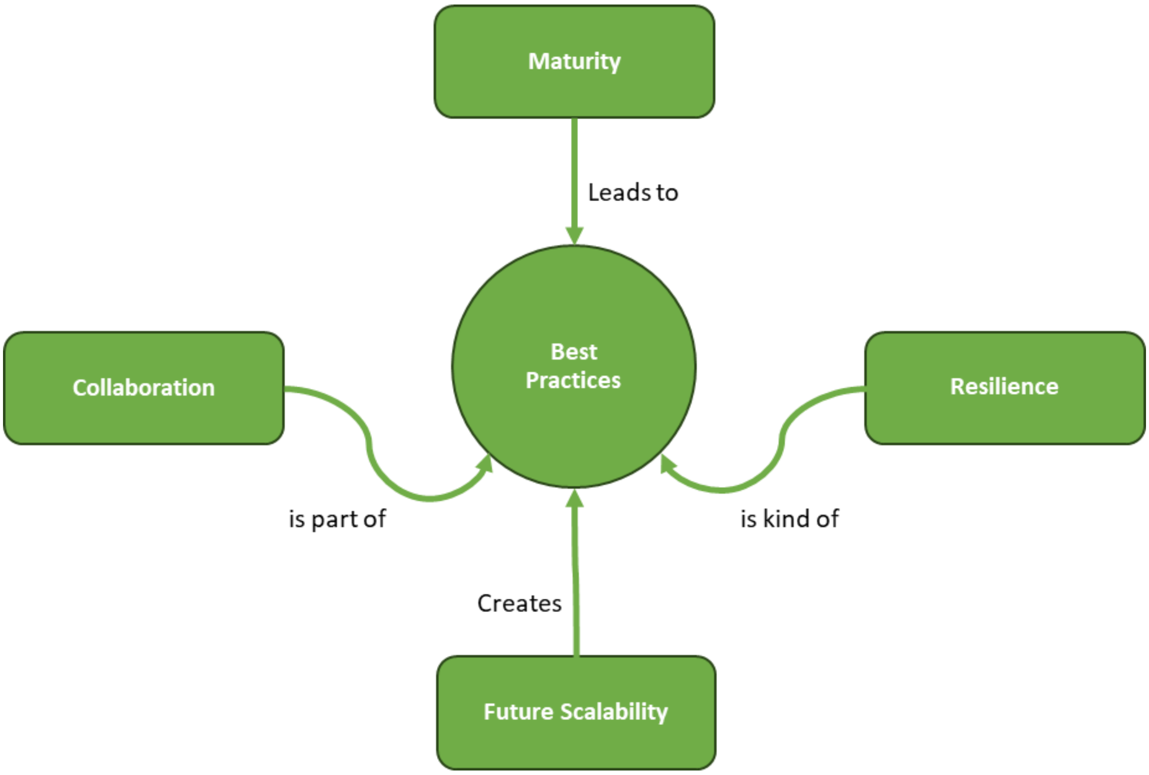


Figure 4.8 The relationship of Best Practices and other factors.

P4 and P11 recommended that FinTech should evaluate its cyber-maturity using the cybersecurity assessment tool. To aid in the ongoing growth of cyber-maturity, FinTech should embrace an international best practice cybersecurity assessment system and incorporate its implementation into its core business activities, with the goal of gradually increasing the degree of cybersecurity maturity. P1 and P10 suggested establishing a financial Cybersecurity Operations Centre (CSOC) for the financial sector and promoting collaboration between the financial CSOC and the national/international similar bodies.

With regards to **Third Parties**, it is clear that they carry a potential threat which is present to organisations' financial information as they would have access to privileged systems. P10 mentions, "I see it's not secure to have a third party." P14 agrees with the same point as he mentions that if dealing with third parties, "CBB mandates to adhere some precautions", in which he suggests that FinTech organisations need to "maintain CBB regulations, and ensure compliance with its rulebooks in terms of dealing with external vendors". But P14 has also brought up the incentive to connect with other third parties as it would be vital for providing services and support in the technology system.

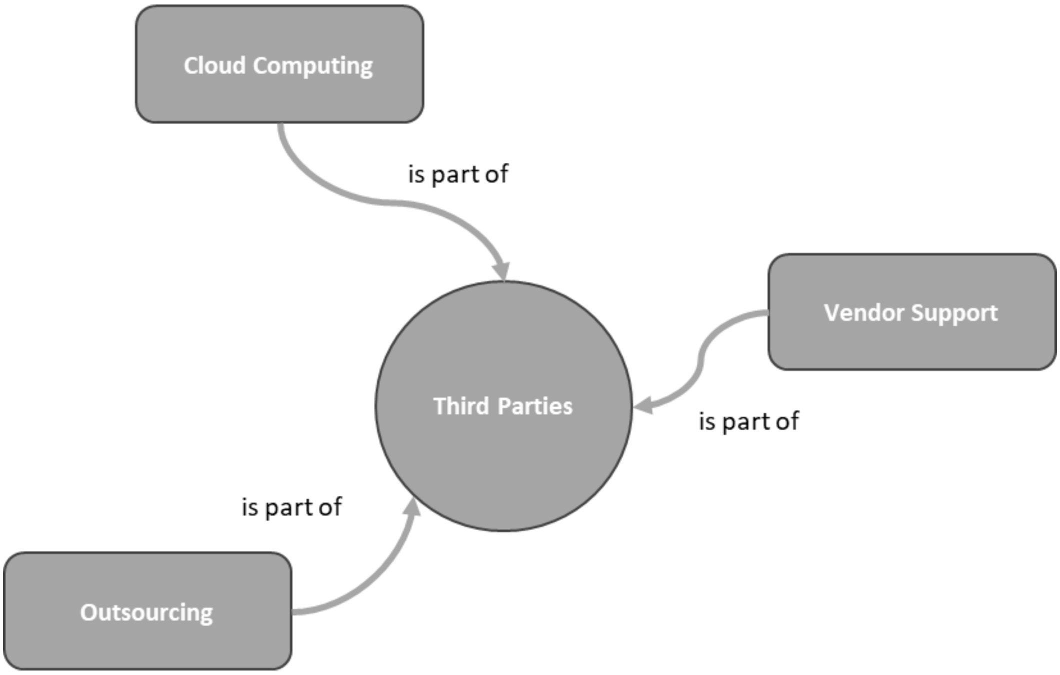


Figure 4.9 The relationship of Third Parties and other factors.

Furthermore, as the discussion about third parties goes deeper, there is an issue regarding outsourcing financial organizations and potential threats to financial data security. It's important to mention that when organisations outsource certain software and services built by third parties, this could lead organisations to experience financial data breaches and other adverse events. P2, P8, and P14 have clearly explained how cloud outsourcing functions in terms of how it hires a third party to provide services needed for the FinTech organisation. P2 mentions how beneficial and "cost-effective" outsourcing is, while both P8 and P14 remark how cloud outsourcing has evolved in terms of cloud security and how it plays a crucial role in terms of providing services in organisations.

4.4.1.5. Building Structures:

This stage entails assembling sets of patterns into an organised structure that represents a thorough depiction of the proposed cybersecurity framework. The process of building structures, or the analysis that precedes their development, entails a careful sequence of processes such as cutting, pasting, combining, triangulating, and assembling (LeCompte, 2000). The process of structural analysis may be enhanced by the use of visual representations. According to (Miles & Huberman, 1984), researchers possess knowledge that is limited to what they can effectively present via visual means. Doodling serves as a first approach to generating visual representations, such as diagrams, conceptual maps, taxonomic trees, flow charts, and causal maps, with the purpose of illustrating the relationships and connections among various patterns.

To generate a comprehensive view of the cybersecurity controls for financial institutes, groupings of patterns discovered in step 4.4.1.4 were combined to create the structure of a framework. As a result, the most significant revision of the risks and cybersecurity controls was the grouping of the 36 items into six main themes (principles) shown in Figure 4.10.

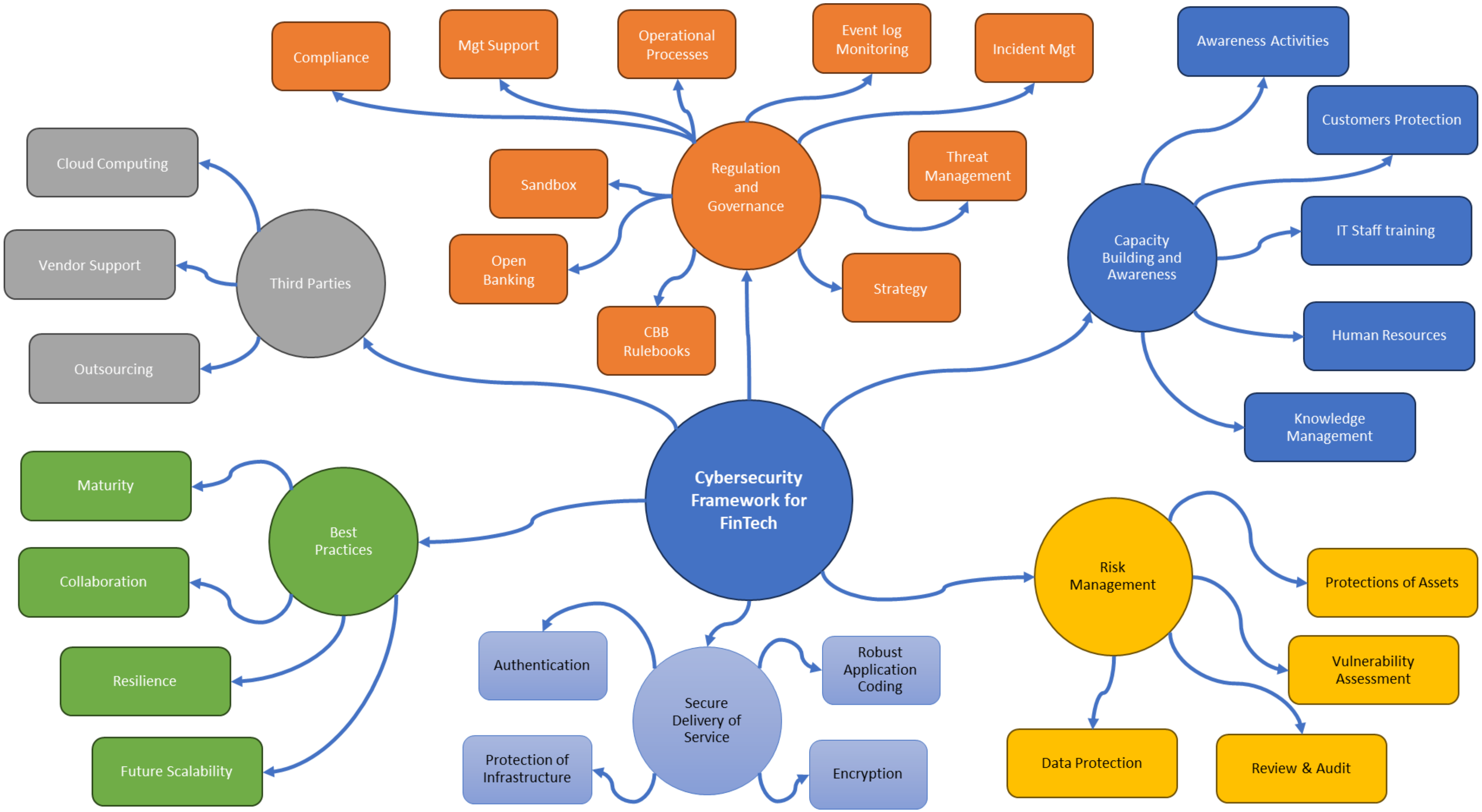


Figure 4.10 The Relationships of the Resulted Themes and Patterns.

Composing such a framework may assist stakeholders in better understanding how to address issues, enhance activities, evaluate their efficacy, or build evidence to explain what occurred. The relationships between the patterns are shown (Figure 4.11) using conceptual maps generated by Nvivo software.

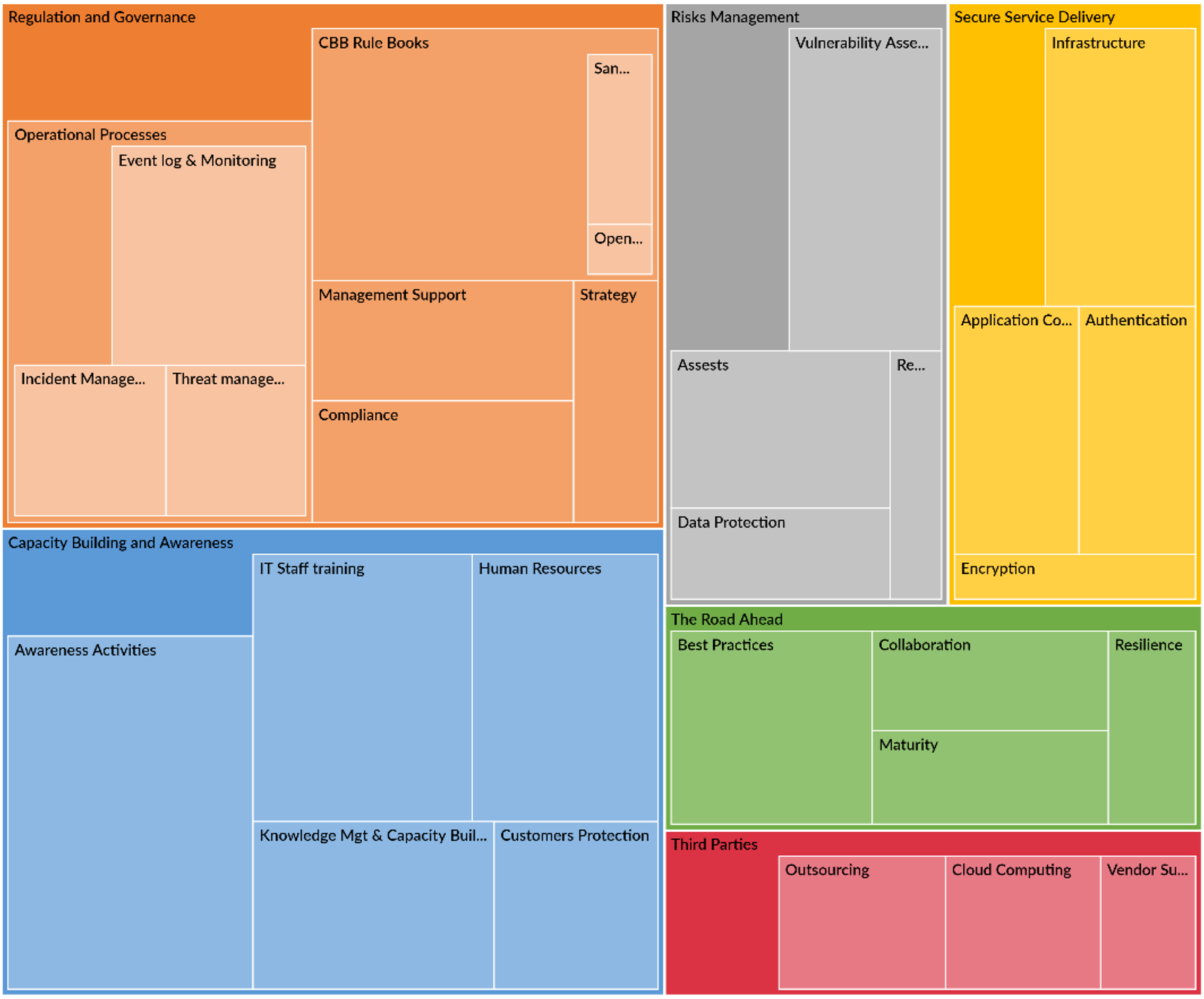


Figure 4.11 The relationships between the patterns.

The total weight of each factor was estimated by the weight focus given by respondents throughout interview talks in terms of word count as listed in Table 4.4.

The empirical findings helped the researcher refine the theoretical framework to make them more applicable to the FinTech environment while also supporting them. Respondents placed a lot of focus on FinTech’s considerable regulation and governance, capacity building and awareness of security measures.

Therefore, six themes and 36 supporting patterns were obtained from the analysis data collected from the sample groups. Table 4.6 lists the common themes and supporting patterns that emerged from the analysis of the 14 semi-structured interviews. Participants contributed to 592 quotes that were directly linked with the relevant codes and main research themes.

Table 4.6 The Resulted Themes and Supporting Patterns that Emerged from the Analysis.

Themes	**Codes**	**Ref.**	**%**
1. Regulation and Governance	11	173	29.22
2. Capacity Building and Awareness	6	154	26.01
3. Risk Management	5	85	14.36
4. Secure Service Delivery	5	76	12.84
5. Best Practices	5	60	10.14
6. Third Parties	4	44	7.43
Totals	**36**	**592**	**100**

Figure 4.12 depicts the percentage coverage of the resulting themes and key cybersecurity principles. As can be observed, Regulation and Governance and People's Capacity Building and Awareness have the most significant influence on the distribution of cybersecurity controls. The greatest level of knowledge and skill necessary is the ability to manage risks, compliance, and security.

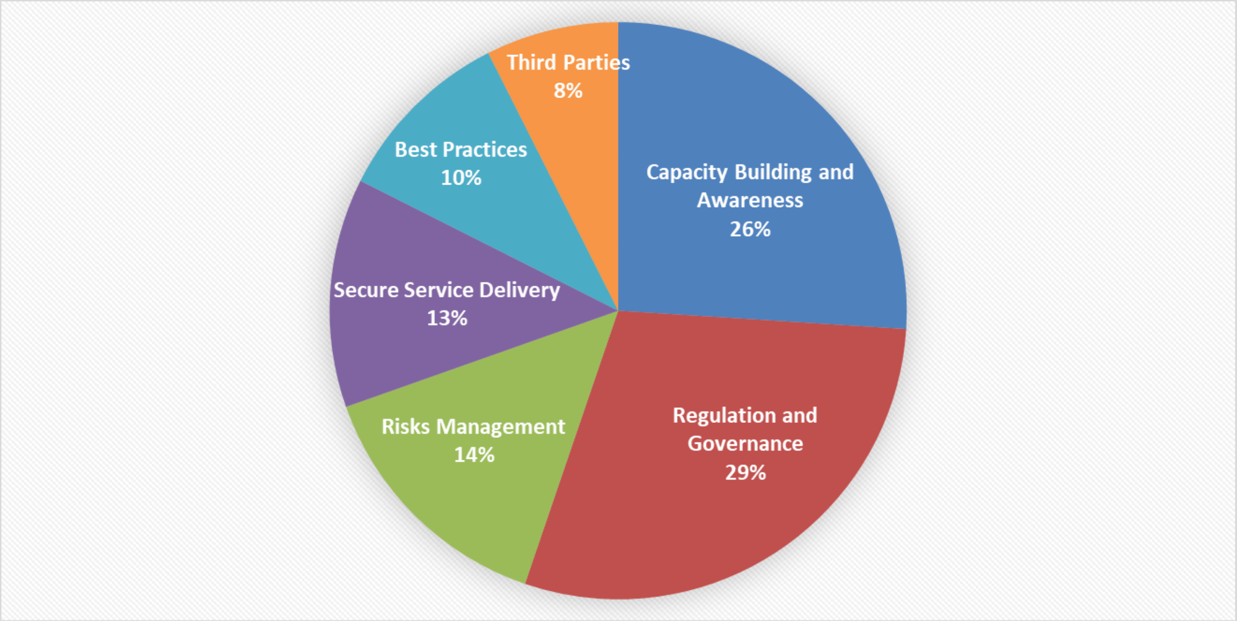


Figure 4.12 Resulting themes.

4.4.2. Themes and Principles Relationships

Spradley's (Spradley, 1979) semantic relationships, often called Ethnosemantic Analysis, is a conceptual model created by James Spradley, an anthropological, for examining the significance and relationship between words within a specific context. It offers an organised method for recognising how individuals classify and link various ideas or elements depending on their understandings and knowledge. This paradigm has gained extensive use in the fields of linguistic anthropology, ethnography, and qualitative research with the purpose of investigating the cultural significances and knowledge structures of diverse groups (Parfitt, 1996). In this section, the relationships between resulted themes and principles are explained using Spradley semantic approach.

4.4.2.1. Regulation and Governance

Regulation and governance influence and set guidelines for risk management in FinTech companies, ensuring compliance with regulatory requirements and promoting risk mitigation strategies. Moreover, it guides Secure Service Delivery by establishing standards and protocols for secure transactions, data protection, and customer privacy in FinTech services. It establishes Best Practices for FinTech operations, such as customer onboarding, fraud prevention, and regulatory reporting. Additionally, it may involve engagement with Third Parties, such as regulatory bodies, auditors, or compliance consultants, to ensure adherence to regulations and governance standards. Figure 4.13 illustrates the relationship between Regulation and Governance and the other principles.

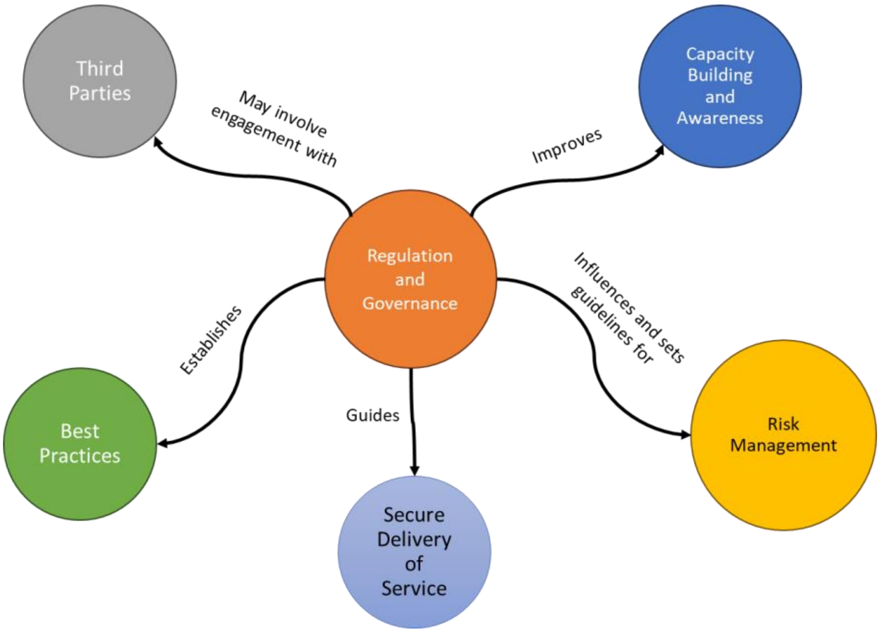

Third Parties
May involve engagement with
Capacity Building and Awareness
Improves
Regulation and Governance
Establishes
Influences and sets guidelines for
Best Practices
Guides
Risk Management
Secure Delivery of Service

Figure 4.13 Relation of Regulation and Governance with Other Principles.

4.4.2.2. Capacity Building and Awareness

Capacity Building and Awareness supports the implementation of Regulation and Governance by providing training and education to FinTech professionals on regulatory requirements and compliance measures. Furthermore, it enhances Risk Management capabilities by equipping FinTech organisations with the knowledge and skills to identify, assess, and mitigate risks effectively. Also, it promotes knowledge and understanding of Best Practices specific to the FinTech industry, including cybersecurity, data privacy, and ethical considerations. It plays a vital role in collaboration with Third Parties, such as industry associations, academic institutions, or training providers, for capacity-building initiatives and knowledge sharing. These relationships with other principles are shown in Figure 4.14.

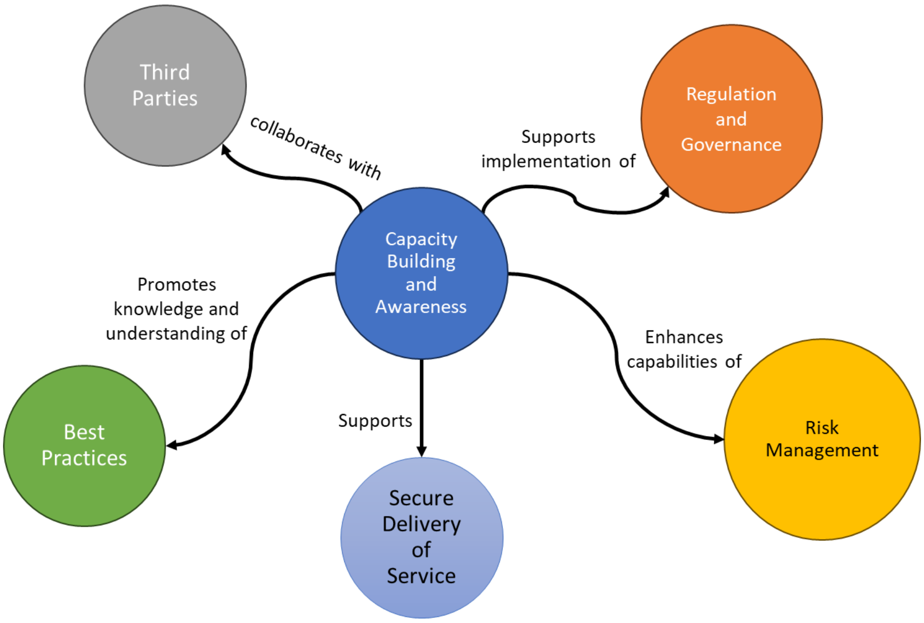

Third Parties
collaborates with
Supports implementation of
Regulation and Governance
Capacity Building and Awareness
Promotes knowledge and understanding of
Enhances capabilities of
Best Practices
Supports
Risk Management
Secure Delivery of Service

Figure 4.14 Relation of Capacity Building and Awareness with Other Principles.

4.4.2.3. Risk Management

Risk management is implemented based on guidelines from Regulation and Governance to ensure compliance and mitigate risks inherent in FinTech operations. In addition, it supports Secure Service Delivery by identifying and assessing potential risks related to transaction security, data breaches, or system vulnerabilities and implementing risk mitigation strategies.

Moreover, it is informed by Best Practices in risk identification, assessment, and mitigation techniques specific to the FinTech sector. It may require the involvement of Third Parties, such as risk assessment firms or cybersecurity experts, to provide specialised expertise or conduct independent risk assessments. Figure 4.15 depicts the above relationships.

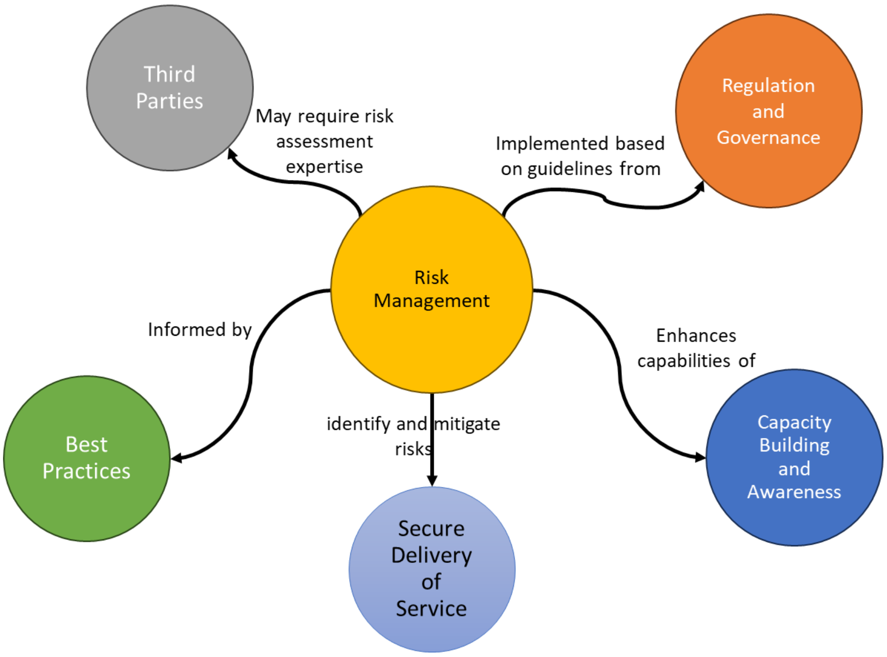

Third Parties
May require risk assessment expertise
Implemented based on guidelines from
Regulation and Governance
Risk Management
Informed by
Enhances capabilities of
Best Practices
identify and mitigate risks
Capacity Building and Awareness
Secure Delivery of Service

Figure 4.15 Relation of Risk Management with Other Principles.

4.4.2.4. Secure Service Delivery

As illustrated in Figure 4.16, Secure Service Delivery adheres to regulations and governance requirements, ensuring that FinTech services are provided in a secure and compliant manner. It mitigates risks identified through Risk Management practices, implementing robust security measures for data protection, transaction integrity, and customer trust. Furthermore, it incorporates Best Practices for security measures, including encryption, access controls, user authentication, and fraud detection systems. Also, this may involve Third Parties, such as payment processors, identity verification providers, or cloud service providers, in service delivery processes while ensuring secure and reliable operations.

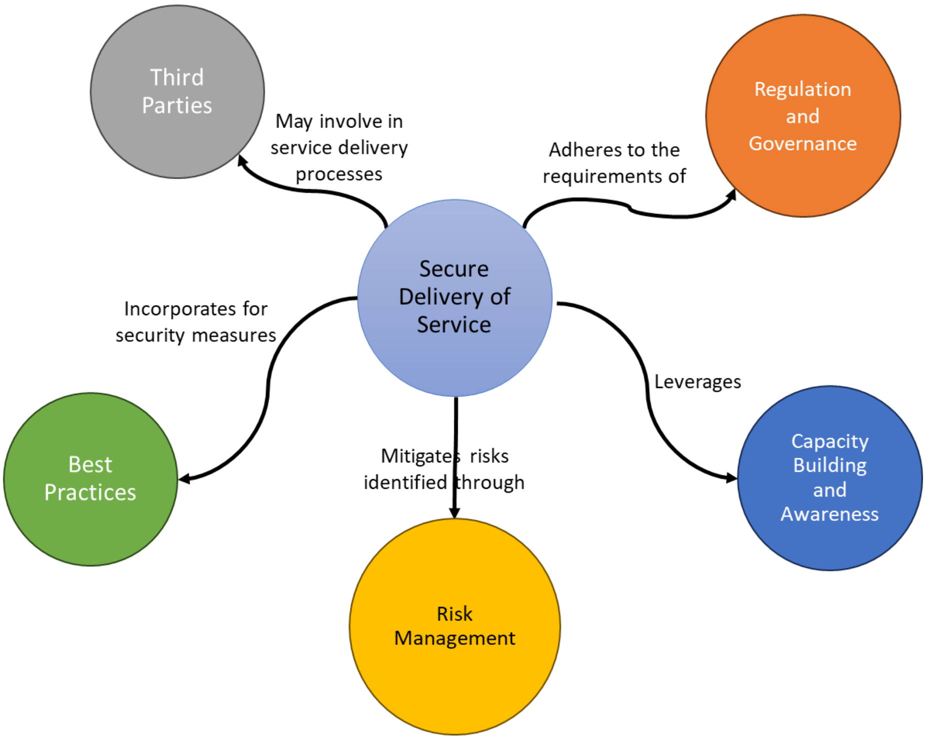

Third Parties
May involve in service delivery processes
Regulation and Governance
Adheres to the requirements of
Secure Delivery of Service
Incorporates for security measures
Leverages
Best Practices
Mitigates risks identified through
Capacity Building and Awareness
Risk Management

Figure 4.16 Relation of Secure Service Delivery with Other Principles.

4.4.2.5. Best Practices

This principle is informed by Regulation and Governance, encompassing industry-specific regulations, guidelines, and standards to optimise operations, risk management, and customer protection in the FinTech space, as shown in Figure 4.17. It Enhances Risk Management and security measures for Secure Service Delivery by incorporating proven methodologies and approaches. It may be shared or adopted by Third Parties, such as FinTech startups or service providers, to improve their practices and align with industry standards and expectations.

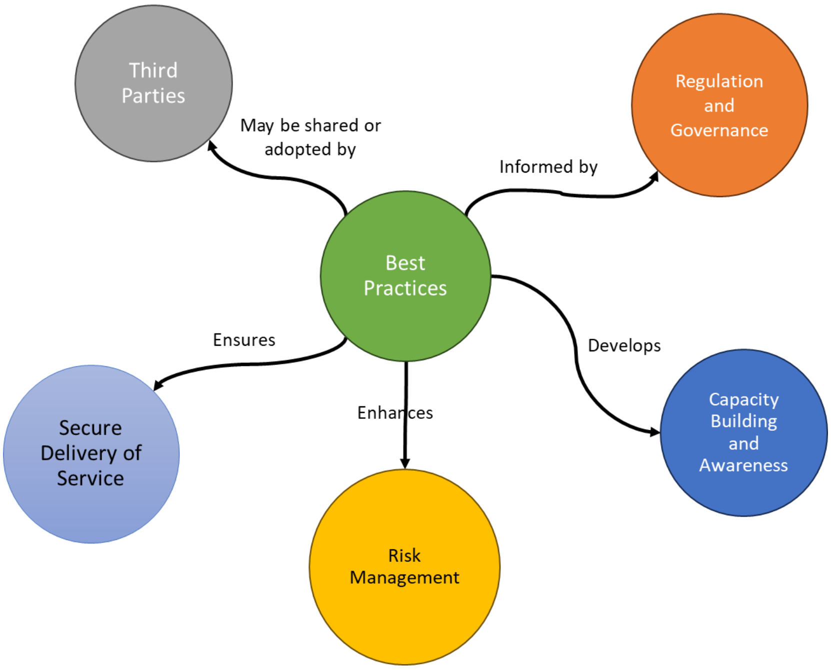

Third Parties
May be shared or adopted by
Regulation and Governance
Informed by
Best Practices
Ensures
Develops
Secure Delivery of Service
Enhances
Capacity Building and Awareness
Risk Management

Figure 4.17 Relation of Best Practices with Other Principles.

4.4.2.6. Third Parties

Third Parties play a vital role in securing FinTech from cyber threats. Within the proposed framework, it can be subject to regulations and governance requirements, especially if they provide services or collaborate with FinTech companies. Moreover, they collaborate with FinTech firms for Capacity Building and Awareness initiatives, offering expertise, resources, or training to enhance cybersecurity knowledge and skills. Additionally, they are involved in Risk Management processes by providing expertise, such as risk assessment, compliance audits, or cybersecurity services, to support FinTech companies in managing risks effectively. They also adopt or adhere to Best Practices in their operations or interactions with FinTech organisations to ensure alignment with industry standards and regulatory expectations. The relationships are shown in Figure 4.18.

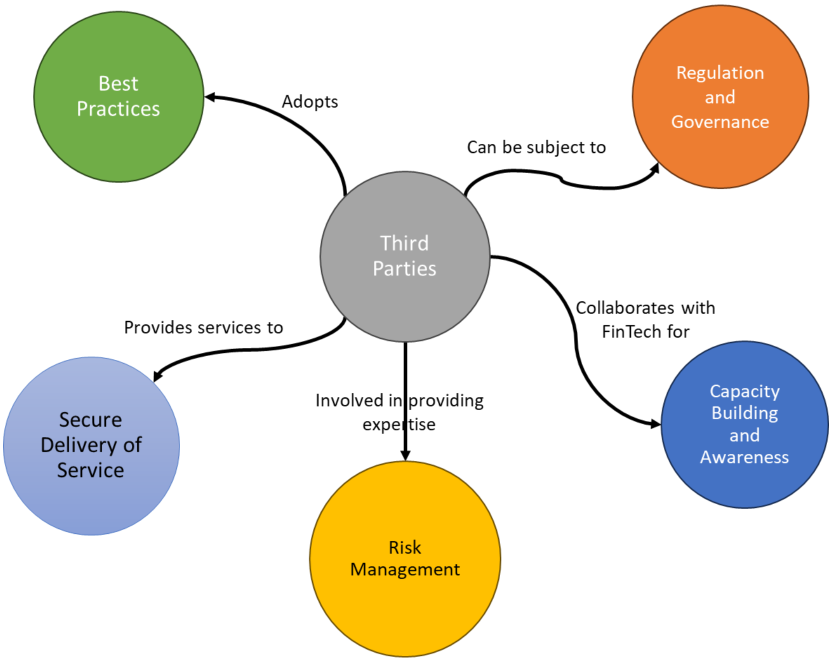

Best Practices
Adopts
Regulation and Governance
Can be subject to
Third Parties
Collaborates with FinTech for
Provides services to
Capacity Building and Awareness
Secure Delivery of Service
Involved in providing expertise
Risk Management

Figure 4.18 Relation of Third Parties with Other Principles.

4.5. The Development of Cybersecurity Framework

The development of a cybersecurity framework for FinTech involved the following results and findings from:

- Based on the STS theoretical framework’s attributes.
- Interviews with higher executives, cybersecurity experts, management leaders, and financial industry professionals.
- A thematic analysis of current cybersecurity standards and frameworks, with a particular emphasis on those mentioned by stakeholders.
- A set of guidelines published by CBB in the rulebook of cybersecurity policies.

The STS Theory illustrates the interconnection of social and technological elements inside a system. Let's analyse how the stated elements align with this framework:

The advantages of employing a Socio-technological Systems (STS) approach lie in its capacity to offer a holistic perspective for protecting FinTech systems. By addressing both the social and technological dimensions of cybersecurity, this approach leads to a stronger and more resilient defence. It improves the user's experience and promotes a culture of cybersecurity awareness among the FinTech institution and important stakeholders. By incorporating these components using a sociotechnical perspective, FinTech firms may implement a complete cybersecurity framework that promotes a secure setting for financial transactions and safeguards sensitive client information.

FinTech, due to its inherent characteristics, involves handling sensitive financial information and needs strong cybersecurity measures. Table 4.7 illustrates the way the STS components we previously mentioned are applied to the research themes for the FinTech cybersecurity framework.

Table 4.7 Research Themes mapped to STS Framework.

Structure: • **Regulation and Governance:** This defines the organizational structure for cybersecurity, including roles, responsibilities, and reporting lines. • **Best Practices:** These established procedures define how work activities are carried out securely within the organization. • **Third-Party Management:** This establishes the structure for collaboration and information exchange with external vendors.	**Technology:** • **Secure Service Delivery:** This encompasses the technological infrastructure, software, and tools used to provide secure financial services. • **Risk Management:** This involves technical tools and processes for identifying vulnerabilities within the system.
Actors: • **Employees:** They play a crucial role in implementing security practices and adhering to policies. Training and awareness programs are vital for this group. • **Customers:** Their behavior can be influenced by security education to minimize risks like phishing attacks. • **Third-Party Vendors:** They are actors who interact with the system and need to adhere to data security protocols.	**Work Activities:** • **Capacity Building and Awareness:** These activities involve training programs for employees and customers on secure practices. • **Risk Management:** This includes activities like security assessments, vulnerability scanning, and incident response procedures. • **Secure Service Development:** This involves activities like secure coding practices, data encryption, and access control implementation.

The progressive results achieved through the research journey of developing the cybersecurity framework explicitly tailored for the FinTech industry in Bahrain can be observed through Figure 4.19. In Figure 4.11, a conceptual map is presented, showcasing the relationships between various patterns. This map is generated using Nvivo software and serves as a visual representation of the interconnectedness of these patterns. Moving to Figure 4.12, the focus shifts to the percentage coverage of the resulting theme and fundamental cybersecurity principles, as indicated by the interviews' participants. This figure provides insight into the significance and prevalence of these principles within the study context. Figure 4.20 presents the culmination of this progression, where a comprehensive framework is presented. This framework consists of six principles that establish crucial cybersecurity goals for FinTech firms to implement and achieve. Alongside these principles, Figure 4.20 includes a list of recommended controls, which offer further guidance and direction for effective cybersecurity implementation. Together, these Figures (4.11, 4.12, 4.20) showcase the progression of the framework's development, starting from a conceptual map and culminating in a comprehensive set of principles and controls for cybersecurity in Bahrain’s FinTech industry.

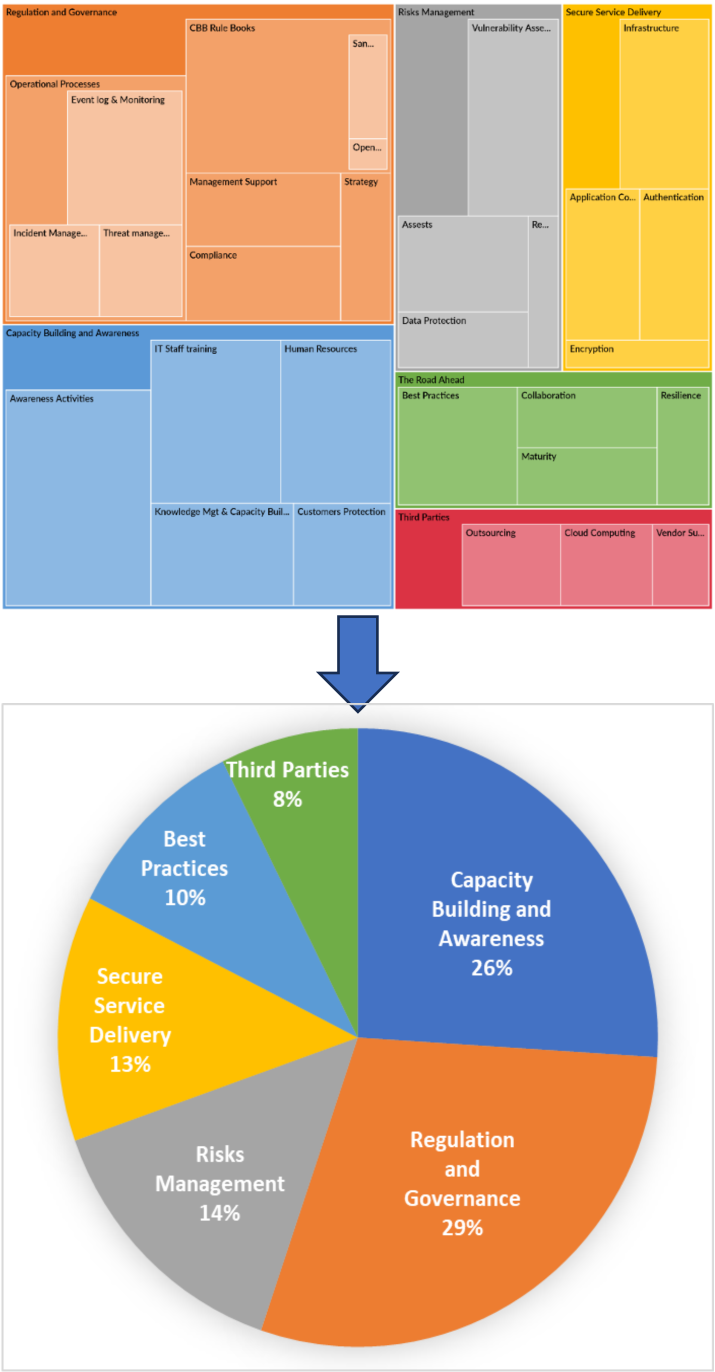


Figure 4.19 The progressive journey of developing the cybersecurity framework.

The framework was built around six principles concepts, which are shown in Figure 4.20.

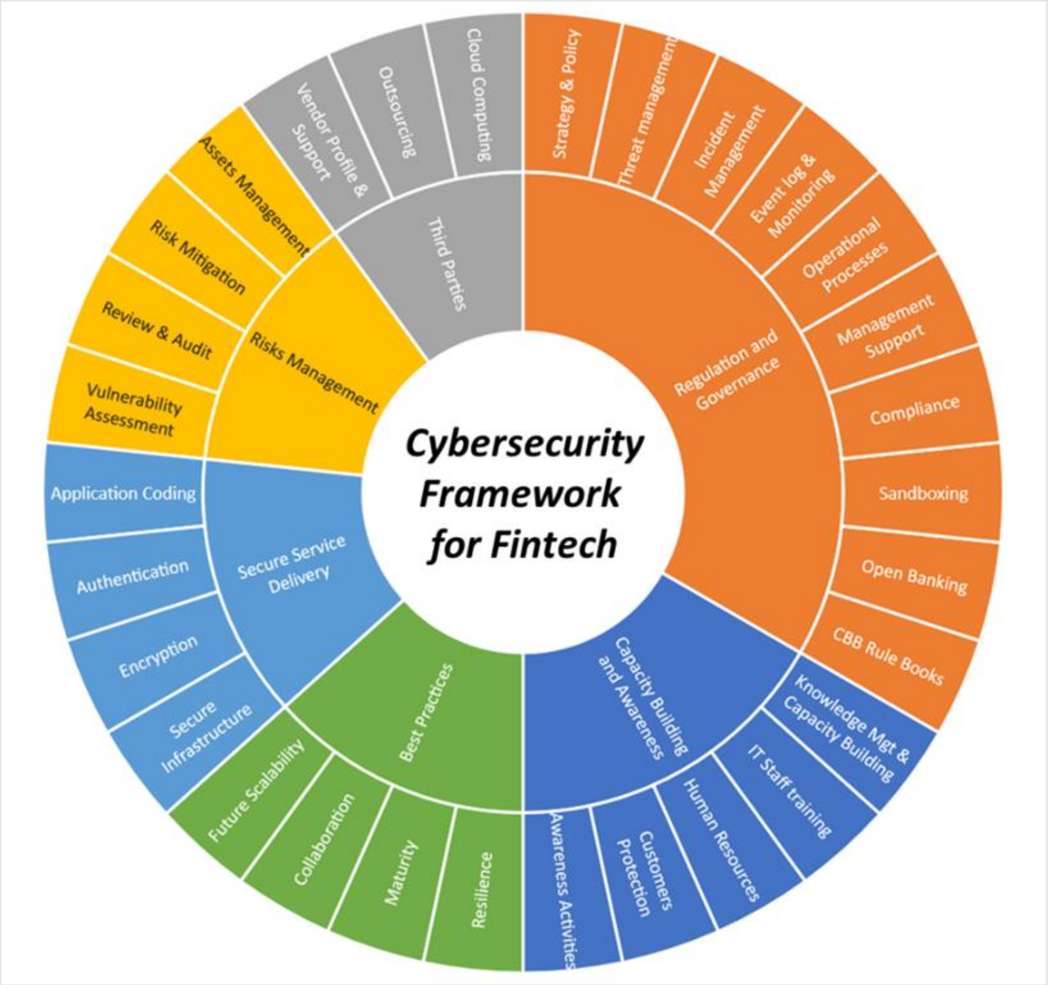


Figure 4.20 The resulting Cybersecurity Framework for Bahrain's FinTech.

The proposed cybersecurity framework for Bahrain's FinTech entities is presented in this section.

4.5.1. Principles of Cybersecurity Framework for FinTech

Cybersecurity is not simply an internal concern for FinTech; financial regulatory and supervisory bodies must mandate certain principles for all financial sector stakeholders to guarantee the security of services and the protection of customers.

The proposed six principles are intended to help FinTech stakeholders in Bahrain, including regulatory and supervisory authorities, to improve their supervisory guidelines, policy measures, and cooperation on issues related to FinTech services, with a focus on addressing cybersecurity challenges. The principles outline the conditions that must be met by FinTech innovations and are meant to aid regulatory authorities in their oversight of FinTech firms in Bahrain. The principles affect Bahrain's financial stakeholders, as shown in Table 4.8.

Table 4.8 The principles affecting Bahrain's financial stakeholders.

Principles	**Relevant Stakeholders**
1. Regulation and Governance	CBB, Banks, FinTech
2. Capacity Building and Awareness	FinTech, Banks, Customers, CBB, BIBF
3. Risk Management	FinTech, Banks, Customers, Telecom, Regulators, CBB, BIBF
4. Secure Service Delivery	Telecom, FinTech, Banks
5. Best Practices	Regulators, FinTech, Banks
6. Third Parties	FinTech

The framework is built upon a set of fundamental principles, which implies that it establishes essential cybersecurity goals for FinTech firms to implement and accomplish. The list of recommended controls offers further guidance and directions.

4.5.1.1. Regulation and Governance

Developing and maintaining regulatory standards that FinTech must follow; informing and assisting them in demonstrating compliance with the regulatory ecosystem; adapting regulations to dynamic environments; using principle-based techniques; and controlling the protection of financial infrastructure in general.

4.5.1.2. Capacity Building and Awareness

Establishing dedicated cybersecurity educational programmes, increasing training opportunities, implementing international certification standards, and supporting innovation and development are all examples of good practices and effective strategies.

4.5.1.3. Risks Management

Internal controls and procedures that offer effective enterprise-wide risk management for protected service provision are used to ensure that the integrity of FinTech's services is protected and safeguarded.

4.5.1.4. Secure Service Delivery

FinTech must understand the service delivery channels and infrastructure that connect customers to financial providers, as well as ensure that private information and transaction integrity are preserved. Maintaining the confidentiality of customer data, identifying customers, and guaranteeing their successful authentication throughout client onboarding and transactions are all critical aspects of the secure delivery of FinTech's services.

4.5.1.5. Best Practices

Ensure that FinTech service's security is maintained when new threats develop; ensure that regulatory bodies are aware of both current risks and their strategies to mitigate them; Audit on a regular basis and ensure that all reporting obligations are satisfied, among other things.

Assuring that action is performed in collaboration with external partners, working with several national cybersecurity authorities, exchanging information about threats and events, and ensuring that FinTech firms have suitably trained human resources to deal with cyber threats.

4.5.1.6. Third Parties

Assuring that partners are committed via the proper business processes without jeopardising the security of FinTech's customers or its business.

4.5.2. Cybersecurity Framework Controls:

The framework encompasses various elements to address the sector's specific needs as shown in Table 4.9. It covers areas such as awareness activities, IT staff training, knowledge management, capacity building, regulation and governance, secure service delivery, secure application coding, authentication, encryption, secure infrastructure, risk management, assets management, risk mitigation, review and audit, vulnerability assessment, third parties, cloud computing, outsourcing, vendor profile and support, future scalability, collaboration, maturity, and resilience. The framework comprises six principles and involves thirty control activities, adopting a risk-based methodology to address current and future technological advancements and potential threats.

Table 4.9 Cybersecurity Framework Controls

Principle	**Controls**	
Capacity Building and Awareness	Awareness Activities	Customer Protection
	IT Staff training	Human Resources
	Knowledge Mgt & Capacity Building	
Regulation and Governance	CBB Rule Books	Management Support
	Open Banking	Incident Management
	Sandboxing	Threat Management
	Compliance	Event Log and Monitoring
	Operational Processes	Strategy & Policy
Third Parties	Cloud Computing	Vendor Profile & Support
	Outsourcing	
Risks Management	Assets Management	Review & Audit
	Risk Mitigation	Vulnerability Assessment
Secure Service Delivery	Application Coding	Encryption
	Authentication	Secure Infrastructure
Best Practices	Future Scalability	Maturity
	Collaboration	Resilience

4.6. Detailed Framework’s Controls and Insights

Table 4.10 presents a detailed exploration of the controls and insights within the proposed cybersecurity framework. It includes a comprehensive list of the controls recommended within each framework principle, addressing various aspects of cybersecurity in Bahrain's FinTech industry.

Table 4.10 Detailed Framework's controls and Insights.

Principle	Controls	Description	Insights
Capacity Building and Awareness	Awareness Activities	They involve disseminating information, materials, and resources to educate stakeholders about various aspects of the FinTech industry, such as Cyber threats, regulatory changes, emerging risks, and best practices.	Awareness activities help in building a shared understanding and knowledge base among individuals and organisations involved in the FinTech sector. These activities may include workshops, seminars, webinars, conferences, and campaigns aimed at increasing awareness and promoting knowledge sharing.
	IT Staff training	IT staff training is an integral part of Capacity Building and Awareness efforts, particularly in the technology-driven FinTech industry.	IT staff training focuses on enhancing the technical skills, knowledge, and expertise of IT professionals working in FinTech organisations. Training programs may cover areas such as cybersecurity, data protection, software development, emerging technologies, and regulatory compliance specific to the FinTech sector. By investing in IT staff training, organisations can strengthen their technical capabilities, improve system security, and ensure compliance with industry standards and regulations.
	Knowledge Management & Capacity Building	Knowledge management involves the systematic collection, organisation, and dissemination of information, best practices, and lessons learned within the FinTech industry. Capacity building focuses on developing the skills, competencies, and capabilities of individuals and organisations to apply knowledge and address industry challenges effectively.	Knowledge management initiatives, such as knowledge-sharing platforms, repositories, and communities of practice, facilitate the exchange of information and experiences, leading to enhanced capacity and continuous learning within the FinTech ecosystem.
Regulation and Governance	CBB Rule Books	CBB Rule Books are regulatory frameworks created and enforced by central banks or regulatory authorities. These rule books establish specific requirements and guidelines for the FinTech industry to ensure the security and integrity of operations.	The regulations outlined in CBB Rule Books cover various aspects of cybersecurity, such as data protection, security controls, incident reporting, and customer protection. Compliance with CBB Rule Books

			is essential for FinTech organisations to meet regulatory obligations, safeguard customer data, and maintain trust in the financial system.
	Open Banking	Open Banking refers to the practice of securely sharing customer financial data between financial institutions and authorised third-party providers with the customers' consent. It aims to foster innovation, competition, and better customer experiences in the financial industry.	They ensure that data privacy, security, and customer protection are maintained throughout the implementation of Open Banking and sandboxing.
	Sandboxing	Sandboxing, on the other hand, involves creating isolated environments for testing and validating new technologies and applications without posing a risk to the production environment.	Regulatory frameworks help establish standards, requirements, and controls to address the potential risks associated with these practices and ensure their compliance with applicable laws and regulations.
	Compliance	Compliance refers to adhering to applicable laws, regulations, and industry standards regarding cybersecurity in the FinTech sector. Regulatory frameworks set requirements for data protection, security controls, incident reporting, and customer protection.	Regulation and governance provide the foundation for establishing and enforcing compliance requirements. They define the regulatory landscape, establish the necessary controls and processes, and oversee compliance efforts to ensure that FinTech organisations meet the required standards and fulfil their regulatory obligations.
	Operational Processes	Cybersecurity operational processes encompass the day-to-day activities and procedures involved in managing and protecting FinTech's information systems and data. These processes include vulnerability management, incident response, access control, and network monitoring,	Compliance with regulatory frameworks ensures that Cybersecurity operational processes align with the necessary security controls, incident management procedures, and risk mitigation strategies defined by the governing authorities.
	Strategy & Policy	Cybersecurity strategy and policies provide a plan for managing and mitigating cybersecurity risks within FinTech firms. The strategy outlines the FinTech's long-term goals, risk appetite, and strategic initiatives to protect its systems and data. Policies, on the other hand, define specific guidelines, procedures, and controls that employees must follow to ensure compliance and protect against cyber threats.	This control influences the development and implementation of cybersecurity strategies and policies. They provide the regulatory requirements, industry standards, and best practices that organisations must consider while formulating their strategies and policies. Adhering to regulatory guidelines ensures that the organisation's strategy and policies align with the necessary security measures and compliance obligations mandated by the governing authorities.
Third Parties	Cloud Computing	Cloud computing uses distant servers on the Internet for storing, managing, and processing data rather than depending on local servers or desktop systems.	Involves ensuring that the cloud service provider has robust security measures in place, such as encryption, access controls, regular security updates, and incident response capabilities. FinTech organisations must carefully select and assess cloud service providers, establish service

			level agreements (SLAs) that include security requirements, and regularly monitor and audit the provider's security practices, maintaining the confidentiality, integrity, and availability of customer data.
	Outsourcing	Outsourcing is the practice of assigning specific corporate operations or responsibilities to external third-party suppliers or service providers.	The vendor's security profile, including its policies, procedures, incident response capabilities, and data protection measures, should align with the FinTech organisation's security requirements. Establishing contractual agreements that define security responsibilities, data protection, and breach notification processes is crucial in managing the cybersecurity risks associated with outsourcing.
	Vendor Profile & Support	Vendor profile and support refer to the assessment and management of third-party vendors in terms of their cybersecurity capabilities and support.	Includes ongoing support and collaboration to address potential cybersecurity issues. This includes engaging with vendors to remediate vulnerabilities, receive security updates and patches, and establish effective communication channels for incident response. Regular communication, monitoring, and periodic assessments of vendor security practices are essential to ensure that third-party vendors align with the FinTech organisation's cybersecurity requirements and contribute to overall risk mitigation efforts.
Risks Management	Assets Management	Assets management involves identifying, classifying, and understanding the critical assets and information systems within an organisation. In the context of cybersecurity, assets can include customer data, financial records, intellectual property, infrastructure, and software applications.	By understanding the value and importance of assets, risk management helps prioritise the allocation of resources and security measures to protect them effectively. It ensures that appropriate controls and safeguards are in place to minimise the risk of unauthorised access, data breaches, or loss of critical assets.
	Risk Mitigation	Risk mitigation is the process of identifying, evaluating, and implementing measures to reduce or eliminate potential risks.	Once risks are identified, risk management strategies and techniques are employed to mitigate those risks. This can include implementing security controls, encryption, access management, intrusion detection systems, and incident response plans. Risk management ensures that appropriate measures are in place to address identified risks effectively, reducing the likelihood and impact of cybersecurity incidents.

	Review & Audit	Regular reviews and audits help evaluate the effectiveness of existing security measures, policies, and controls. They involve assessing compliance with regulatory requirements, industry standards, and internal policies.	Through audits, risk management ensures that security controls are implemented correctly, gaps are identified, and appropriate remediation measures are taken to address any identified shortcomings. It helps organisations maintain continuous improvement in their cybersecurity practices and align with industry best practices.
	Vulnerability Assessment	Vulnerability assessment is the process of identifying and evaluating vulnerabilities in FinTech systems, networks, and applications. It involves conducting comprehensive scans and tests to identify potential weaknesses that can be exploited by cyber threats.	It facilitates the identification and prioritisation of vulnerabilities based on their potential impact and likelihood of exploitation. By assessing vulnerabilities, risk management enables FinTech firms to focus their resources and efforts on addressing the most critical risks first. It helps in determining appropriate remediation measures, such as patching systems, implementing secure configurations, and conducting regular vulnerability scans to maintain a robust cybersecurity posture.
Secure Service Delivery	Application Coding	Application coding refers to the process of writing and developing software applications.	Secure coding principles and techniques help prevent vulnerabilities and weaknesses that could be exploited by attackers. By following secure coding practices, such as input validation, proper error handling, and secure data storage, FinTech businesses can reduce the risk of security breaches and ensure the integrity and confidentiality of customer data.
	Authentication	Authentication is the verification of the identity of individuals or systems trying to gain entry to resources or services.	Implementing multi-factor authentication, biometrics, or other robust authentication methods helps ensure that only authorised individuals or systems can access sensitive financial services. By integrating robust authentication protocols and mechanisms, FinTech organisations can prevent unauthorised access, protect customer accounts, and maintain the confidentiality and integrity of transactions and sensitive information.
	Encryption	Encryption involves converting data into an unreadable form using cryptographic techniques.	Encryption plays a vital role in protecting data both in transit and at rest. By encrypting sensitive data, such as customer information, financial transactions, and communication channels, FinTech companies can safeguard the confidentiality and integrity of data. Secure service delivery includes the implementation of robust encryption algorithms

			and protocols to ensure that data remains secure even if it is intercepted or accessed by unauthorised parties.
	Secure Infrastructure	Secure infrastructure encompasses the fundamental hardware, software, and network elements that facilitate the provision of FinTech services.	Having a secure infrastructure is paramount. This involves setting up reliable firewalls, intrusion detection and prevention systems, protected network setups, and consistently applying security updates and fixes. By establishing a secure infrastructure, FinTech innovations can protect against unauthorised access, network attacks, and other cybersecurity threats. Secure service delivery encompasses the implementation and maintenance of a secure infrastructure that forms the foundation for the secure operation of FinTech services.
Best Practices	Future Scalability	Future scalability refers to the ability of a cybersecurity framework or practice to adapt and accommodate future growth and changes in the FinTech organisation.	Involve adopting scalable solutions that can accommodate increased data volumes, additional users, and emerging technologies without compromising security. By considering future scalability, FinTech organisations can proactively plan and implement security measures that can grow and evolve alongside their business, minimising the need for significant security overhauls in the future.
	Collaboration	Collaboration refers to the act of working together with internal stakeholders, industry peers, regulatory bodies, and other relevant entities to enhance cybersecurity in the FinTech sector.	It enables the sharing of threat intelligence, best practices, and lessons learned. By collaborating with others, FinTech firms can gain insights into emerging threats and vulnerabilities, access specialised expertise, and collectively address common security challenges. Collaboration can take the form of participating in industry associations, sharing information with trusted partners, engaging in knowledge-sharing forums, and actively contributing to the development of industry standards and guidelines.
	Maturity	Maturity in the context of cybersecurity best practices for FinTech refers to the level of development and effectiveness of the FinTech security program.	Maturity in cybersecurity means that FinTech has a well-defined and documented approach to security, with clear roles and responsibilities and a focus on continuous improvement. By aiming for maturity, FinTech entities can better protect their systems and data, detect and respond to security incidents, and adhere to regulatory requirements.

	Resilience	Resilience refers to the ability of a FinTech organisation to withstand and recover from cybersecurity incidents or disruptions effectively.	Includes implementing proactive measures such as robust backup and disaster recovery plans, incident response plans, and regular testing and validation of these plans. Resilience also involves establishing redundant systems, maintaining up-to-date patches and security updates, and conducting regular vulnerability assessments. By focusing on resilience, FinTech organisations can minimise the impact of cybersecurity incidents, reduce downtime, and maintain the continuity of their services, thereby protecting their reputation and customer trust.

4.7. Summary

This study developed a framework for cybersecurity measures for Bahrain FinTech companies. The following precise research question was addressed in this chapter: identifying the factors that influenced the development of a cybersecurity framework. Simultaneously, to fulfil research questions and objectives, the outcomes of data collection and the qualitative interviews have been aggregated to analyse and validate the findings of the interviews systematically. This provided insights into the main principles of the cybersecurity framework, along with common cybersecurity recommendations to support FinTech by protecting them from cyber risks. Furthermore, the research work looked at aspects at both the human and organisational levels that influence the cybersecurity framework for financial entities.

Over the course of four months, the 14 interviews in this multiple-case study lasted around 13 hours in total. Each interview was automatically transcribed by MS Teams, producing a total of 14 files of discussion transcript. The initial findings provide a detailed explanation of how various levels of cybersecurity experts in Bahrain's financial institutions incorporate thoughts to answer the research question investigating critical factors for the development of a cybersecurity framework for FinTech stakeholders in Bahrain, as well as recommendations for improvements.

Participants address several areas that leverage the establishment of an efficient cybersecurity framework for FinTech. It must take into account various aspects such as cyber risks, technology, people, and processes.

FinTech in Bahrain should prioritise establishing dedicated cybersecurity educational programmes, increasing training opportunities, implementing international certification standards, and supporting innovation and research.

During interviews and discussions with the experts, they confirmed the importance of regulation and governance in developing and maintaining regulatory standards that FinTech must follow, informing and assisting FinTech in demonstrating compliance with the regulatory ecosystem, adapting regulations to a dynamic environment, using principle-based techniques; and controlling the protection of financial infrastructure in general.

FinTech firms must understand the service delivery channels and infrastructure that connect customers to financial providers, as well as ensure that private information and transaction integrity are preserved. Maintaining the confidentiality of customer data, identifying customers, and guaranteeing their successful authentication throughout client onboarding and transactions are all critical aspects of the secure delivery of FinTech's services.

Participants agreed that FinTech must declare any issue when a cyber threat attack occurs, ensuring that regulatory bodies are aware of both current risks and their strategies to mitigate them. Controls must be performed in collaboration with external partners, ensuring that FinTech firms work with several national cybersecurity authorities, exchange information about threats and events, and have suitably trained human resources to deal with cyber threats.

In this chapter, the empirical findings from the research were presented, focusing on the interconnections between technology, people, and processes in the FinTech cybersecurity context. By analysing data through an STS lens, this chapter reveals patterns, relationships, and themes that contribute to cybersecurity controls within the industry. Building on the research findings, the STS theoretical model facilitated the synthesis of the knowledge gained to develop a comprehensive cybersecurity framework for the FinTech industry. The framework emphasises the importance of considering technology, people, and operational factors in an integrated manner.

It is suggested that the proposed framework should be further reviewed, validated, and tested for its applicability with a few FinTech stakeholders in Bahrain. The researcher intends to hold a focus group discussion and a Delphi session for a group of FinTech and cybersecurity experts and conduct rounds of discussions to review, validate, and test the applicability of the proposed framework.

This page intentionally left blank

Chapter 5: Framework Validation and Refining

5. Chapter 5: Framework Validation and Refining

5.1. Framework Final Design

The core contribution of this research lies in the proposed cybersecurity framework for FinTech in Bahrain, which addresses the unique characteristics and challenges of the FinTech industry. The framework encompasses key elements such as Regulation and Governance, Capacity Building and Awareness, Risk Management, Secure Service Delivery, Best Practices, and Third Parties.

The qualitative data analysis conducted in Chapter 4 resulted in the research themes mapped to the STS framework as illustrated in Table 4.7. The analysis demonstrates that human capital is a critical asset in the complex landscape of the FinTech socio-technical system. FinTech, by its nature, deals with sensitive financial data and requires robust cybersecurity controls. Principles and controls resulting from the data analysis fall smoothly with the STS theoretical framework, as either social or technical components. Here how these components were translated into a FinTech cybersecurity framework:

5.1.1. Social Components

Compliance with Regulations and Governance, such as the CBB rulebook or the PCI DSS standard, shapes data security policies and access controls. Clear governance structures define cybersecurity roles and responsibilities within FinTech institutions. Moreover, Capacity Building and Awareness sessions and training workshops for employees on phishing attacks, password hygiene, and data security protocols, for instance, facilities prevent social engineering attacks. In addition, educating FinTech customers about secure online practices strengthens the overall security posture. Implementing industry Best Practices and standard security measures like multi-factor authentication becomes part of the culture of FinTech institutes. Sharing best practices with stakeholders ensures consistent security across Bahrain's FinTech ecosystem.

Third Parties, such as cloud computing providers and other vendors and partners, should have adequate security measures in place. An outline of risk management processes, cybersecurity expectations and responsibilities is done via contractual agreements to ensure the protection of FinTech systems.

5.1.2. Technical Components

Deploying firewalls, intrusion detection systems, and data encryption mechanisms are all examples of Secure Service Delivery to protect sensitive information within FinTech systems Moreover, to minimise application and software exploits, secure coding practices and vulnerability management processes are implemented. It is vital to conduct regular Risk Management and cybersecurity assessments, to identify and prioritise potential threats. Business continuity and disaster recovery plans ensure service availability in case of cyberattacks. Leveraging technology effectively by selecting tools that complement team capabilities enhances cybersecurity measures. Furthermore, adapting to the technology changes by staying agile in response to regulatory, customers' needs, and threat landscape shifts.

5.1.3. The Interaction of Framework's Themes

The interaction of technology, people, and organizational structure is complicated. For instance, Regulations enhance secure service delivery by mandating specific encryption protocols for financial data. Moreover, capacity-building programs train employees on secure coding practices and data breach response procedures. Best practices for third-party APIs can minimise vulnerabilities in integrations with external financial services.

Implementing sophisticated cybersecurity solutions and processes may require teams to modify their operational and communication methods. On the other hand, the team's capacity and expertise might impact the selection of technology. For example, a team that possesses extensive data analytics skills is more likely to utilise solutions that facilitate sophisticated threat intelligence analysis.

Cybersecurity operational processes and activities are also influenced by wider regulatory changes, technological advances, and evolving cyber threats. These trends have the potential to impact the way FinTech organisation is structured, how decisions are made, and the dynamics inside teams. Furthermore, the conduct of both internal and external stakeholders, including clients, staff, and third parties, has a substantial impact on the social environment in which cybersecurity functions.

By comprehending these connectivities, a comprehensive framework for cybersecurity that optimises the capabilities of FinTech human resources while reducing cyber risks was established. A Sunburst diagram, depicted by concentric circles, was used to visualise all these relationships. The chart with multiple levels of categories shows how the outer ring relates to the inner ring. The inner ring in the centre represents the framework's main principles, with the hierarchy moving outward from the centre to the outer ring, which represents the framework's controls. Figure 5.1 shows the visualisation (Sunburst diagram) of the final framework layout, which is named Cybersecurity Framework for FinTech in Bahrain (**CFFB**). It has six principles and 30 controls.

The framework aimed to provide FinTech entities in the early stages of cybersecurity with a comprehensive set of fundamental elements to consider while building their cybersecurity measures. Alternatively, it could serve as a baseline standard for FinTech organisations in more advanced stages of cybersecurity to consistently evaluate and improve the protection of their technology, systems, and practices.

Testing the CFFB might be the first step in determining its applicability and practicality for Bahrain's FinTech innovations. Since each component in the CFFB is a critical element, further validation of the CFFB framework will enable the growth and enhancement of these elements as well as the creation of new tools to support FinTech companies in their pursuit of accurate implementation.

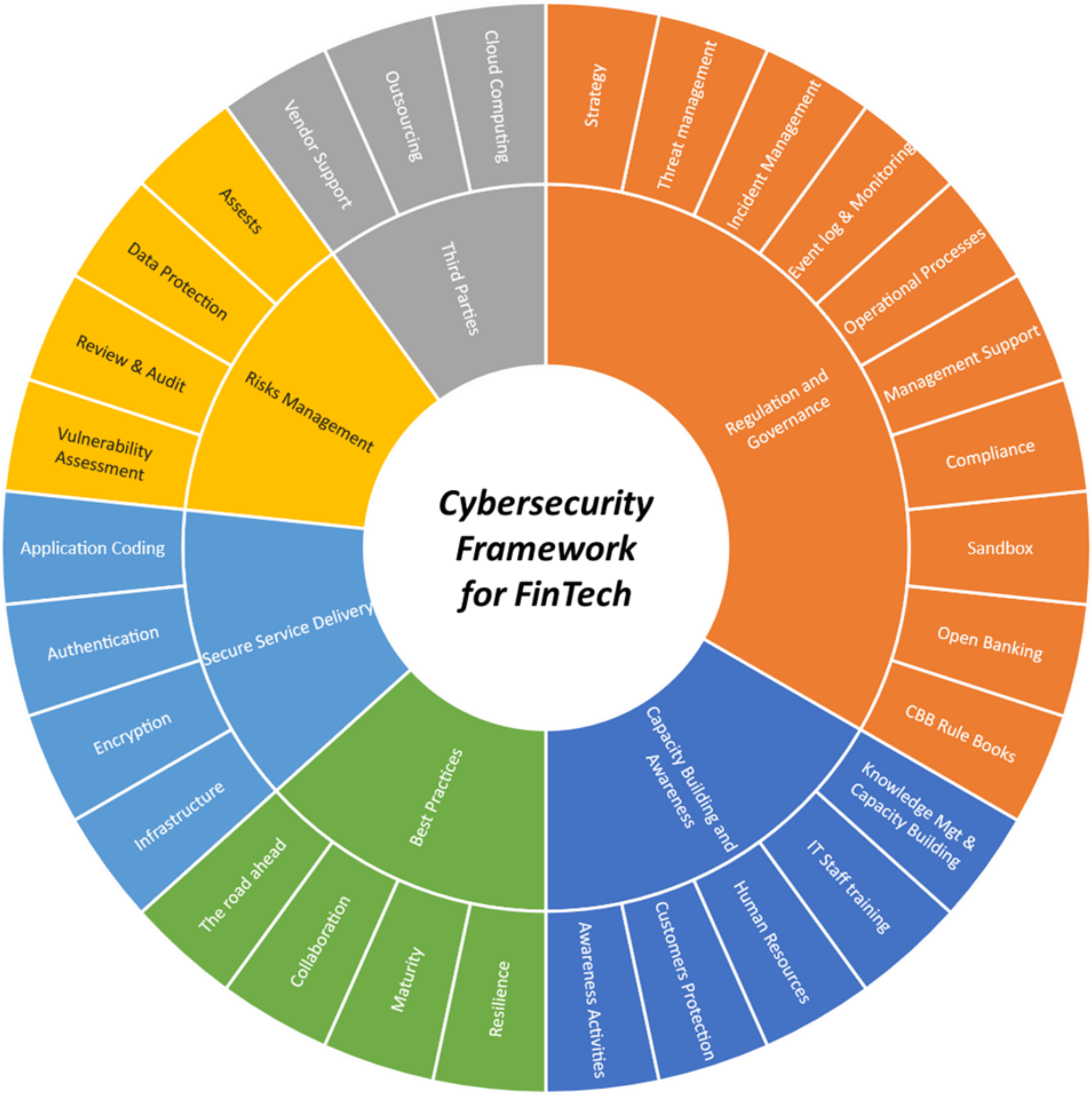


Figure 5.1 The Proposed Cybersecurity Framework for FinTech in Bahrain (CFFB)

This chapter focuses on validating and refining the cybersecurity framework. It evaluates the framework's principles, identifies potential shortcomings, and assesses its ability to enhance the resilience of FinTech enterprises against cyber threats. The goal is to provide practical and effective controls for FinTech firms to mitigate cybersecurity risks, safeguard sensitive financial data, and win the trust of customers and stakeholders.

5.2. Validation of CFFB Framework

Since it is exploratory research, the validation exercise of the proposed framework is essential because it supports the research to ensure that the cybersecurity framework is aligned with financial industry best practices.

Validation of the framework was conducted using an approach of focus group discussion. The research findings and proposed framework were reviewed and validated using a focus group approach. Krueger, a pioneer in the field of focus group discussion technique, recommended that a group of 5-10 members be chosen (Krueger, 2014). Accordingly, a group of six professionals with diverse backgrounds, including cybersecurity consultants, FinTech practitioners, bankers, and academic professionals, were chosen based on their skills, role, and experience. In addition, they possess both academic and practical expertise in cybersecurity for FinTech field. The academic members are essential in a focus group setting since they possess up-to-date knowledge of the most recent studies concerning cybersecurity threats and trends, specifically those related to FinTech. He will evaluate the feasibility of the framework and provide ideas to enhance its efficiency for actual use in FinTech businesses. Furthermore, the academic's presence in the discussion ensures an unbiased perspective, encouraging constructive criticism and facilitating an open exchange of ideas among focus group members. This, in turn, enhances the credibility of the validation process and the final framework.

As discussed in Chapter 3, numerous uses of the Delphi technique are common in qualitative research. The fundamental idea of this method is to get participants' feedback and arrive at a consensus. To provide more precise and realistic results, Delphi studies may be combined with quantitative data gathering and the use of quantitative techniques to analyse data. Triangulation is one of the approaches that may promote the validity of qualitative findings and is one of the methods that was employed in this study (Babazadeh et al., 2022).

The optimal number of Delphi session rounds remains unclear, and it should be emphasised that increasing the number of rounds may decrease response rates (Beiderbeck et al., 2021). The number of cycles in every Delphi process differs, although it rarely exceeds one or two iterations (Rowe & Wright, 1999). The flow chart in Figure 5.2 provides a visual representation of the iterative process of expert review and Delphi rounds, emphasizing the importance of expert feedback and consensus in Delphi approach.

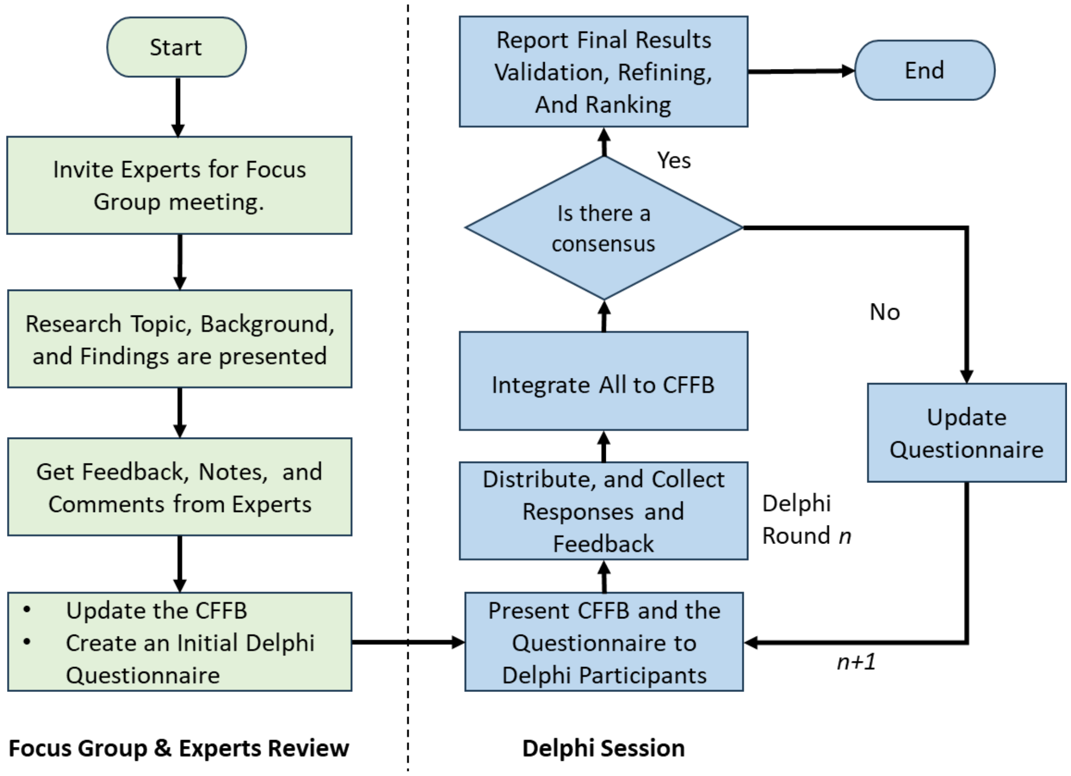

Start
Invite Experts for Focus Group meeting.
Research Topic, Background, and Findings are presented
Get Feedback, Notes, and Comments from Experts
Update the CFFB
Create an Initial Delphi Questionnaire
Focus Group & Experts Review
Present CFFB and the Questionnaire to Delphi Participants
Distribute, and Collect Responses and Feedback
Delphi Round n
Integrate All to CFFB
Is there a consensus
Yes
No
Update Questionnaire
n+1
Report Final Results Validation, Refining, And Ranking
End
Delphi Session

Figure 5.2 Experts Review and Delphi Rounds

5.3. Data Analysis using Delphi Descriptive Statistics.

The data may be analysed in a variety of ways, but in the Delphi method, descriptive statistics are often employed to validate the data collected at each round (Babazadeh et al., 2022). A technique for analysing changes across Delphi rounds is provided by more complex tools like Kendall's W, which was used in this qualitative analysis (Beiderbeck et al., 2021). The Delphi method compares and evaluates experts' responses using descriptive statistics. Responses were quantified using the Likert scale (1-5), and the concordance of feedback and the convergence produced by the Delphi rounds were determined using Kendall's W coefficient. In Kendall's W, W = 1 stands for full compliance, whereas W = 0 stands for no conformity. Although W is utilised as a comparison indication across different rounds of the Delphi session, there is no universally accepted value for W that indicates an "acceptable" amount of conformity (Babazadeh et al., 2022). SPSS is a powerful and versatile tool for data analysis using Delphi descriptive statistics, to obtain the Kendall's W coefficient.

5.4. Experts Review

Considering the recent development of this topic, Bahrain has limited research and a lack of scientific expertise in this field. In this regard, the focus group technique was utilised to get specialised opinions on providing insights from experts in the field for validating the CFFB framework. The focus group technique has a wide range of uses in qualitative studies besides forecasting the future. The key element of this method is to collect input and come to an agreement among the panellists. A panel of experts is created in this context, and the thoughts gathered in this manner will be highly beneficial since those engaged in this field are well-informed and experts. (Appendix 6)

5.4.1. Experts Details

The panel of experts comprises individuals with extensive expertise in the field of FinTech, banking, and cybersecurity and can provide valuable perspectives on the research. Table 5.1 uses alphanumeric identifiers (Rx) instead of names to illustrate the characteristics of the 6 expert reviewers. Table 5.1 provides a brief characteristics of the group of experts.

Table 5.1 Experts Details

NO	Alias	Line of Business	No Experience Years
1.	R1	FinTech	18
2.	R2	FinTech	22
3.	R3	FinTech	20
4.	R4	Cybersecurity Expert	14
5.	R5	Bank	17
6.	R6	Bank	7

5.4.2. Experts' General Feedback

An open-ended question was used to kick off the discussion in order to get their expectation for a new cybersecurity framework that is currently being researched. The expert members were given the findings of the research as well as the list of derived principles and controls as depicted in Figure 5.1. They were requested to provide their opinions, perceptions, and recommendations that were crucial to the framework but were not stated. The discussion was informative and helpful for getting common notes and remarks, which were mentioned in Table 5.2.

Table 5.2 Expert's General feedback

Notes & Remarks	**Reviewers**
Comprehensive	R1, R2, R3, R4, R5
Prioritisation with the Business	R2, R3, R5
Size of FinTech's Business	R3, R6
Compliance challenges	R2, R3, R5
Essential for cybersecurity baseline	R4, R5, R6
Different risk nature	R1, R3, R5
Bahrain needs this	R1, R2, R3, R4, R5, R6

The table lists common comments made by the participants regarding their general reaction to the proposed framework.

The first comment, "Comprehensive," was made by almost all the participants (R1, R2, R3, R4, and R5) and highlights that the framework provides a holistic approach to cybersecurity for FinTech Innovations in Bahrain. They confirm that all aspects of cybersecurity were covered.

R2, R3, and R5 made the second comment, "Prioritization with the Business," indicating that the cybersecurity framework was aligned with the FinTech business objectives. This proved that a risk-based approach has already been taken to prioritise cybersecurity activities that were most relevant to FinTech businesses.

R3 and R6 highlight the relevance of the size of FinTech businesses to their cybersecurity needs in the third comment, "Size of FinTech's Business. " This suggests that the scale and complexity of FinTech businesses can impact FinTech's cybersecurity requirements, and this framework was designed to cater to FinTech businesses of different sizes.

The fourth comment, "Compliance challenges," was made by R2, R3, and R5, and it validated that the cybersecurity framework is designed to incorporate regulatory compliance requirements, and FinTech companies should be aware of the compliance challenges they face.

Moreover, R4, R5, and R6 agreed that this framework provided a starting point toward implementing robust cybersecurity activities for FinTech, and they highlight that it is "Essential for cybersecurity baseline".

In addition, R1, R3, and R5, in the sixth comment, "Different risk nature," indicate that FinTech businesses face different types of risks compared to traditional financial institutions. They were satisfied with the framework controls that were tailored to address the unique risks faced by FinTech companies.

Finally, all participants (R1, R2, R3, R4, R5, and R6) agreed that Bahrain needs a robust cybersecurity framework for FinTech firms. Bahrain recognised the potential of FinTech and was taking steps to promote its growth and adoption. Such a framework will assist in providing a secure and reliable environment for FinTech businesses to operate in.

5.4.3. Expert Discussion and Suggested Enhancements

To build a structured questionnaire that would be utilised as a tool in the upcoming Delphi session, principles and controls were updated, as shown in Table 5.3. The experts validated the accuracy of the research findings obtained from the interaction and the associated feedback.

Table 5.3 Themes from the discussion

Theme	Main Discussion	Ref
Robust Regulation and Governance	Cybersecurity frameworks should be designed to be effective, efficient, and adaptable. It involves creating a framework of laws, policies, and standards that can effectively address current and future cyber threats.	R1, R5, R6
	It should also be adaptable to changes in technology and the evolving cyber threat landscape. It should also be flexible enough to allow for innovation and the introduction of new technologies.	R2, R6
	Monitoring and logging events can help FinTech detect and respond to cyber-attacks.	R5
Competent People and High	Cybersecurity requires a skilled workforce to design, implement and manage security measures. FinTech that invests in training and development for their cybersecurity staff are better equipped to respond to cyber threats.	R4, R5

Cybersecurity Awareness	Employees must understand the risks posed by cyber threats and be able to recognise suspicious activity. FinTech innovations that prioritise cybersecurity awareness training for all staff are better furnished to prevent cyber-attacks.	R1, R2, R3, R5
	It helps to comply with regulatory requirements and avoid costly data breaches.	R3
Identifying and Managing Cyber Risk	Risk assessment includes identifying possible risks, vulnerabilities, and impacts. The results can help FinTech prioritise their cybersecurity efforts and allocate resources effectively.	R3, R5
	FinTech should implement appropriate security controls to mitigate identified risks.	R4, R5, R6
	Cybersecurity risks are constantly evolving, so FinTech should regularly monitor and assess their risks. This may involve conducting regular risk assessments, monitoring logs and alerts, and staying up-to-date with the latest threats and vulnerabilities.	R5
	Cybersecurity is an ongoing process, and FinTech must remain vigilant and adapt to changing threats over time.	R1, R2
Secure Delivery of Services	FinTech should use secure protocols for delivering services over the Internet.	R1, R2
	Access controls are essential for ensuring that only authorised users have access to services.	R2
	The use of robust encryption algorithms is vital to ensure that data is protected from unauthorised access.	R2
Managing Third Parties	Before engaging with a third-party technology provider, FinTech should conduct due diligence to assess their cybersecurity posture.	R1, R2, R3
	Establish a security requirements list for third-party technology providers, which should be documented in a contract or service level agreement (SLA). FinTech should regularly monitor and audit third-party compliance with security requirements.	R2, R4

	Establish incident response plans that outline the steps to be taken by the third party in the event of a cyber-attack.	R3, R6
	Communication and collaboration between FinTech and its third-party technology providers are essential for effective cybersecurity and to ensure that security risks are identified and addressed in a timely manner.	R2, R3, R5
Adopting Best Practices	A robust cybersecurity framework is developed through a collaborative approach involving stakeholders from banking, government, academia, and civil society. This can help to ensure that the framework is practical, effective, and reflects the needs of all stakeholders involved.	R1, R2, R3

5.4.4. CFFB Framework Refining

Table 5.4 provides a comparison of various principles and controls before and after the changes. The changes are listed alongside the modifications made in the "Notes" column; the main focus of the table is the changes made to the principles of regulation and governance, capacity building and awareness, risk management, third-party management, and best practices.

Under the principle of Regulation and Governance, the "Strategy" control has been renamed "Strategy & Policy." This principle has also undergone a combination of "Event log and monitoring," "Incident Management," and "Threat Management" controls, which are now referred to as "CS Operational Processes." Similarly, "Open Banking" and "Sandboxing" have been combined under the same name.

The "Management Support" control has been deleted, while "Human Resources" has been merged with "Management Support." The "Customers Protection" control has been renamed "Communications," and "Risk Mitigation" has replaced "Data Protection" as the new name.

The "Assets" control has been renamed "Assets Management," and "Vendor Support" has been renamed "Vendor profile & Support." Finally, "The road ahead" control has been renamed "Future Scalability" under the "Best Practices" principle.

Overall, changes have been made to simplify and streamline the principles and controls involved in FinTech's cybersecurity framework. The updated framework is illustrated in Figure 5.3.

Table 5.4 List of control changes

Under Principle	Before	After	Notes
Regulation & Governance	Strategy	Strategy & Policy	Renamed
	• Event log & Monitoring • Incident Management • Threat management	CS Operational Processes	Combined
	• Open Banking • Sandboxing	Open Banking & Sandboxing	Combined
	Management Support		Deleted
Capacity Building and Awareness	Customers Protection	Communications	Changed
	Human Resources	Management Support	Deleted
Risk Management	Assets	Assets Management	Renamed
	Data Protection	Risk Mitigation	Renamed
Third Parties	Vendor Support	Vendor profile & Support	Renamed
Best Practices	The road a head	Future Scalability	Renamed

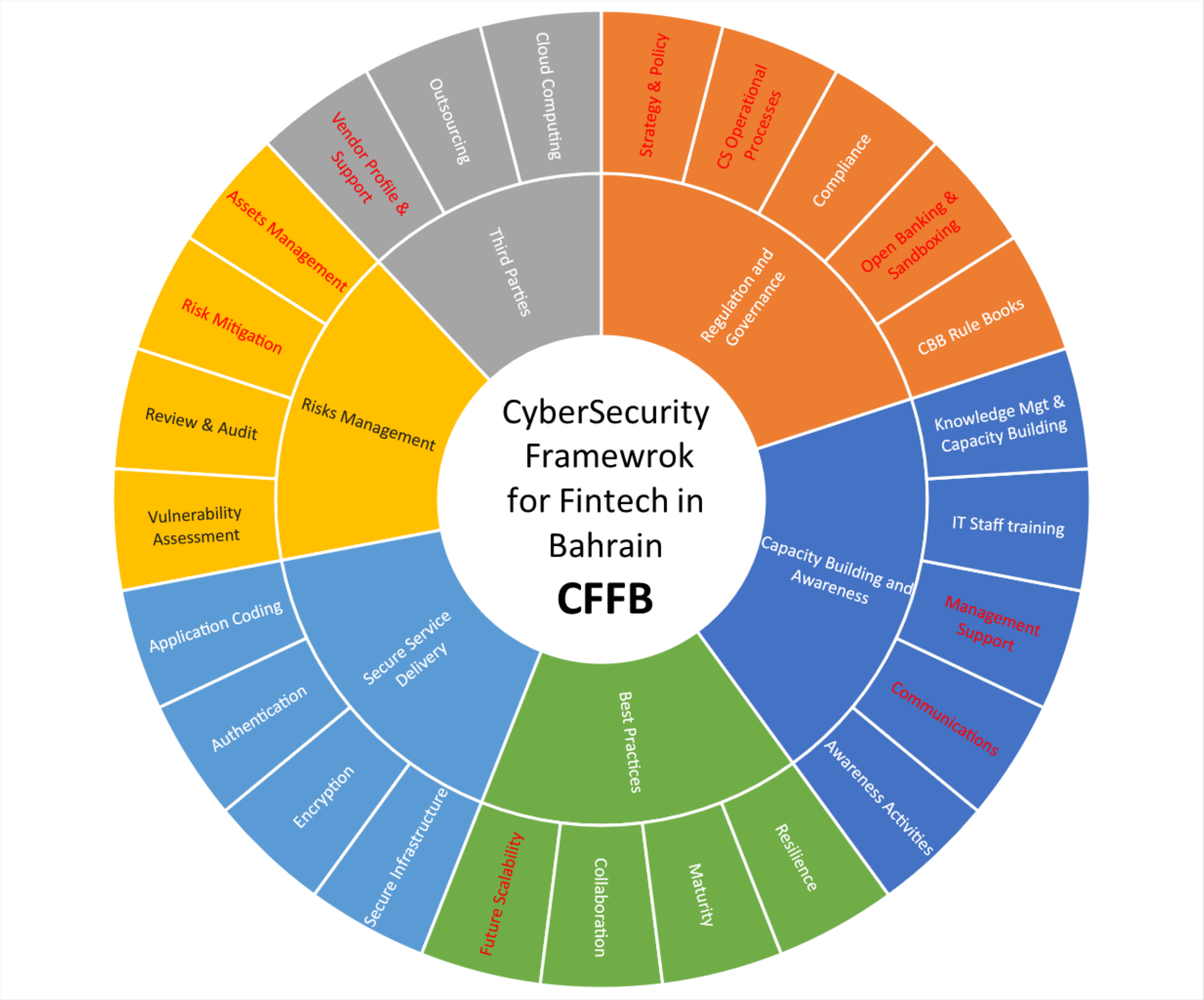


Figure 5.3 Updated CFFB framework.

5.5. Refining and Ranking of the Framework’s Controls.

One approach to getting feedback from stakeholders on the Framework's use today and how it could evolve to address FinTech's future cybersecurity challenges was via a panel discussion. The panel or a workshop is an excellent venue for engagement with FinTech’s stakeholders. Their feedback is essential for the framework's open and transparent validation and for the revision process. This phase will build on top of prior work and findings.

The workshop gave the researcher and other interested parties the opportunity to:

1. Present and share the researcher’s work for the CFFB framework and listen to feedback, notes, and recommendations for improvements.
2. Validate, refine and rank the CFFB’s principles and controls.

3. Find discussion themes in the topic as identified by the panellist and participants.
4. Receive notes in response to the Delphi's survey.

5.5.1. NGN Majlis and the Delphi Session

The researcher collaborated with NGN International to hold a Delphi session at NGN Majlis for a group of FinTech and cybersecurity experts in the financial sector in Bahrain and conduct rounds of discussions that involve a comprehensive evaluation of the framework, providing their opinions, identifying any gaps, or suggest areas for improvements. NGN Majlis is a monthly panel discussion platform for Bahrain’s ICT experts in different Cybersecurity themes. In total, **42** experts attended the NGN Majlis, and 25 of them participated in the Delphi session.

NGN majlis

JOIN US FOR TWO DYNAMIC CYBERSECURITY SESSIONS

Wednesday, May 31th 2023 from 11:00 AM to 2:00 PM (Bahrain Time)
Location: The Ritz-Carlton

EVENT SPEAKERS

Event Moderator: Salah Albenjasim
Cybersecurity Ph.D. Researcher

Alaa AlBahrani
Senior Manager, Information & Cyber Security at Ahli United Bank

Fawaz Ghazal
Chief Executive Officer of FLOOSS

Hasan Muhi
Information Security Management/BCP Officer at KFH

David Bradley
Channel Sales Engineer, Axonius

Figure 5.4 NGN Majlis Panel

NGN majlis
Salah Albenjasim
Cybersecurity Ph.D. Researcher
MODERATOR
Alaa AlBahrani
Senior Manager, Information & Cybersecurity at Ahli United Bank
Fawaz Ghazal
Chief Executive Officer at FLOOSS
Hasan Muhi
Information Security Management/BCP Officer at KFH
NGN majlis

Figure 5.5 NGN Majlis Panel Discussion

5.5.2. NGN Majlis Programme:

Four panel experts from different disciplines in cybersecurity and FinTech businesses (Figure 5.4 and 5.5) run the Majlis's programme as show in Table 5.5. The programme provides attendees with valuable information and insights into the intersection of FinTech and cybersecurity in Bahrain. The panellists and moderator will share their expertise and facilitate discussions to enhance the understanding of the research topic.

Table 5.5 NGN Majlis Event Plan.

Programme	Time (Min)	Panellist
1. Welcome & Introductions of Guest Speakers	5	Moderator: Salah AlBenJasim
2. FinTech in Bahrain	15	Fawaz Ghazal
3. FinTech's Cybersecurity Threats	15	Alaa AlBahrani
4. Cybersecurity Controls and standards	15	Hasan Muhi
5. Cybersecurity Framework for Bahrain's FinTech	15	Salah AlBenJasim
6. Q&A		All
7. Delphi Survey	15	Salah AlBenJasim
8. Results, Summary, and Closing	10	All

5.5.3. Majlis's Participants

Throughout the Majlis session, participants were engaged and active via interactive Q&A, contributing ideas, making comments, and asking questions to the panellists and the researcher. A good turnover of **42** participants participated in the workshop. The workshop's statistical population included financial experts, cybersecurity specialists, and IT professionals who operate in the area of FinTech in Bahrain. Figure 5.6 describes the workshop's participants' descriptive profiles.

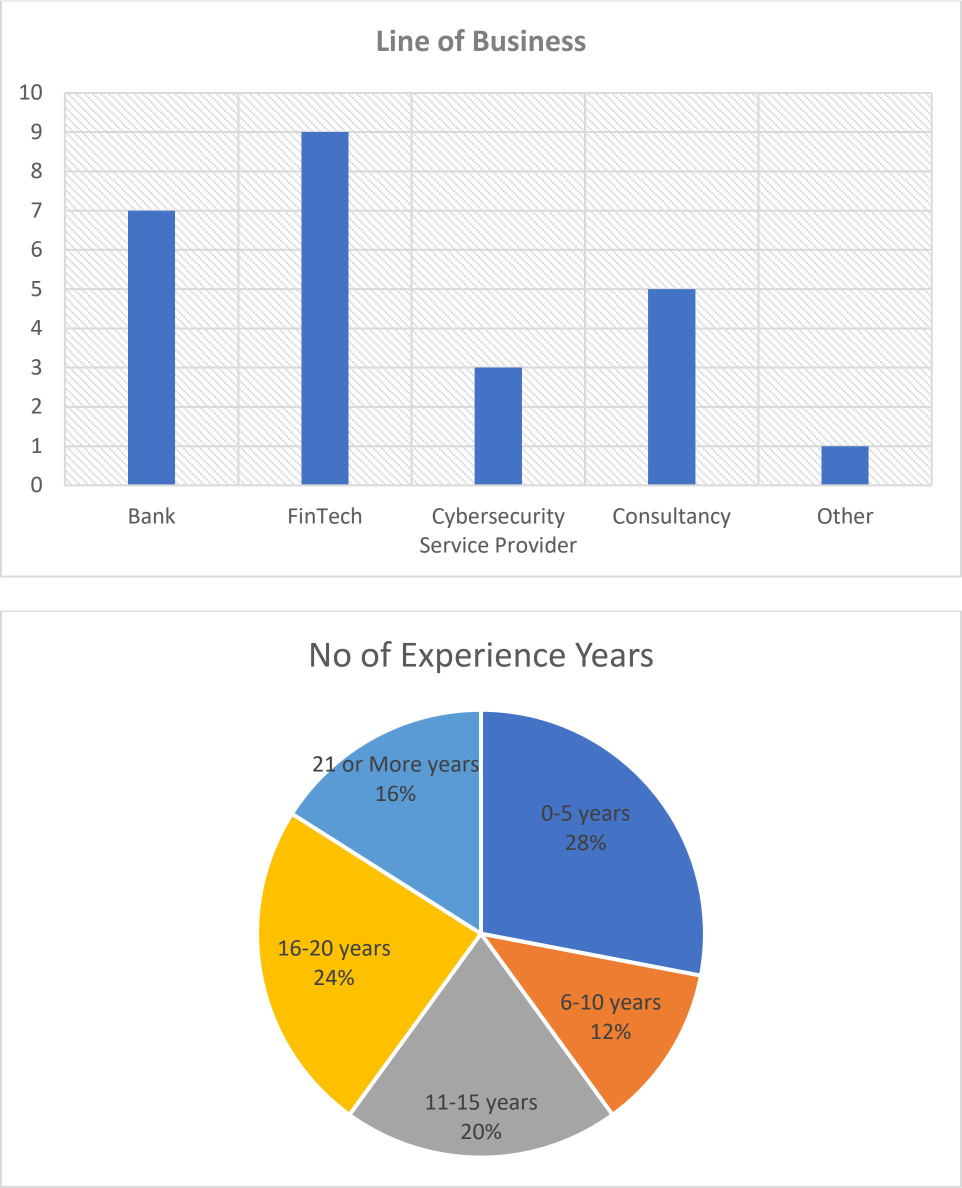


Figure 5.6 Workshop's participants' descriptive profiles.

5.5.4. Majlis Panel Discussion.

The first part of the panel discussion started with an introduction by the researcher highlighting the status of FinTech innovations in Bahrain with open-ended questions for the panellists:

1. *What do you think are the most significant cyber challenges facing FinTech in Bahrain today? How do you suggest addressing them?*
2. *What are some best practices for developing a comprehensive cybersecurity framework for FinTech companies?*
3. *What is the need to have a cybersecurity framework specifically for FinTech in Bahrain?*

Mr. Fawaz Ghazal presents the topic of FinTech in Bahrain, covering its development, current state, and potential future trends. Following that, Alaa AlBahrani discusses cybersecurity threats specific to the FinTech industry, including data breaches, hacking, and identity theft. Hasan Muhi talks about cybersecurity controls and standards relevant to the FinTech sector, focusing on best practices, regulatory requirements, and frameworks for ensuring the security of FinTech systems and data. The first part involves an interactive question-and-answer session where attendees ask questions to the panellists and engage in discussions related to the majlis topics. The outcome of the panel discussion is presented in section 5.6 of this chapter.

5.5.5. Majlis Delphi Session

The researcher handled the second part of the panel discussion. He presents his research's outcomes and the reviewed and updated CFFB (Figure 5.3) and its main components, emphasising that FinTech may use the framework as a guide to assess better, control, mitigate, and interact with cybersecurity risks. It is intended to be a dynamic document that is continuously refined and enhanced. The framework is being developed iteratively, with significant involvement and review from FinTech and cybersecurity experts in Bahrain.

The researcher followed four important Delphi aspects in performing the study: anonymity, iteration, controlled feedback, and statistical aggregation of group answers, as put forth by (Avella, 2016; Rowe & Wright, 1999). Anonymity was maintained by presenting the participants with the group answers without exposing their identities. Participants were also urged not to put their names on the questionnaires in order to preserve their privacy. The Delphi session went through two iterative cycles as shown in Figure 5.2. During these rounds, the framework's controls were modified, followed by a statistical aggregation procedure to determine their final ranks. The participants were provided with controlled feedback. They received the controlled feedback process, which consisted of a well-organized recap of the previous iteration towards the conclusion of each round. Controlled feedback enabled participants to gain insights into the knowledge obtained in the last round, become more problem-solving-focused, provide more accurate comments, and reduce the impacts of noise (Avella, 2016).

5.5.6. Delphi Session – Part 1

Using a structured survey, participants were asked to rank each item on a Likert scale according to its importance (See Appendix 7). Here, instances of consensus and discord are identified, and a forum for identifying new ideas, revising, interpreting, eliminating, and clarifying their benefits and drawbacks is created. In the second round of the survey, identical individuals were asked to rank every control using the Likert scale and assign a weight out of 100% to each control while conveying their thoughts regarding any suggestions or recommendations. Using descriptive statistics, each control's score was computed and then ranked according to its rating. Kendall's W concordance coefficient was derived to figure out the level of consensus among experts.

The Delphi questionnaire (Appendix 7) is designed to capture the following:

1. Ranking the framework's principles according to their importance and priority.
2. Ranking the framework's controls according to their importance.
3. Assign weight to each control out of 100 (%).
4. Receive comments and suggestions that are relevant to Bahrain's FinTech case.

5.5.6.1. Round 1

In the first round of the Delphi session, experts were surveyed in a systematic way and asked to rank each framework's principles on a Likert scale while providing their thoughts on the framework structure and controls. Table 5.6 displays the ranking scores for the main principles.

Table 5.6 Ranking of framework's pillars as a result of Delphi session round one.

Principles	Mean	Std. Deviation	Ranking
1. Risk Management	2.00	1.118	1
2. Regulation and Governance	2.56	1.685	2
3. Capacity Building and Awareness	3.36	1.655	3
4. Secure Service Delivery	3.88	1.364	4
5. Best Practices	4.32	1.464	5
6. Third Parties	4.881	1.130	6

Table 5.7 Analytical statistics for Delphi R1.

N	**25**
Kendall's W	**0.336**
Chi-Square	41.960
df	5
Asymp. Sig.	0.000

According to Kendall's W coefficient of concordance (**W = 0.336**), expert responses have a concordance level of 0.336.

5.5.6.2. Round 2

In the second round, the experts were given a new questionnaire to complete. They were asked to rank the principles of the framework in order of priority while seeing the ranking from the first round that was derived from the average points provided to each principle. The highest priority was given to the value of 1, and the lowest priority to the value of 6. Based on the experts' prioritisation of the six principles throughout this round, Kendall's W coefficient of concordance is computed.

Table 5.8 Prioritizing the importance of the framework's pillars as a result of Delphi round two.

Principles	Mean	Std. Deviation	Prioritising
Risk Management	1.76	0.831	1
Regulation and Governance	2.12	1.269	2
Capacity Building and Awareness	3.32	1.345	3
Secure Service Delivery	3.48	1.194	4
Third Parties	5.08	0.954	5
Best Practices	5.20	1.000	6

Table 5.9 Analytical Statistics for Delphi R2

N	25
Kendall's W	**0.592**
Chi-Square	73.970
df	5
Asymp. Sig.	0.000

Kendall's W in this round was greater (**W = 0.592**). Table 5.8 lists the outcomes of the framework's pillars' prioritisation.

5.5.6.3. Nonparametric Statistical Analysis

The degree of consensus of 0.336 in the first Delphi round and 0.592 in the second round suggested an acceptable agreement amongst the participants on the ranking and prioritising, according to Schmidt's (Schmidt, 1997) interpretation of Kendall's W coefficient. Therefore, the findings of Kendall's W coefficient showed a high level of agreement among the experts, giving confidence in the outcomes and offering a valid justification not to conduct a third round.

This practice not only led to the higher value of consensus and conformity of the cybersecurity framework among the ICT and financial experts but also to the definition and ranking of the framework's pillars and controls according to their significance in the FinTech innovations context, making them more validated and highly accepted. Tables (5.10 and 5.11) summarise the results of the Delphi session rounds.

Table 5.10 Ranking and prioritising of framework's principles as a result of Delphi rounds.

	Delphi Round 1			**Delphi Round 2**		
Principles	Mean	Std. Deviation	Ranking	Mean	Std. Deviation	Prioritising
Risk Management	2.00	1.118	1	1.76	0.831	1
Regulation and Governance	2.56	1.685	2	2.12	1.269	2
Capacity Building and Awareness	3.36	1.655	3	3.32	1.345	3
Secure Service Delivery	3.88	1.364	4	3.48	1.194	4
Best Practices	4.32	1.464	5	5.20	0.954	6
Third Parties	4.881	1.130	6	5.08	1.000	5

Table 5.11 Analytical statistics for Delphi rounds.

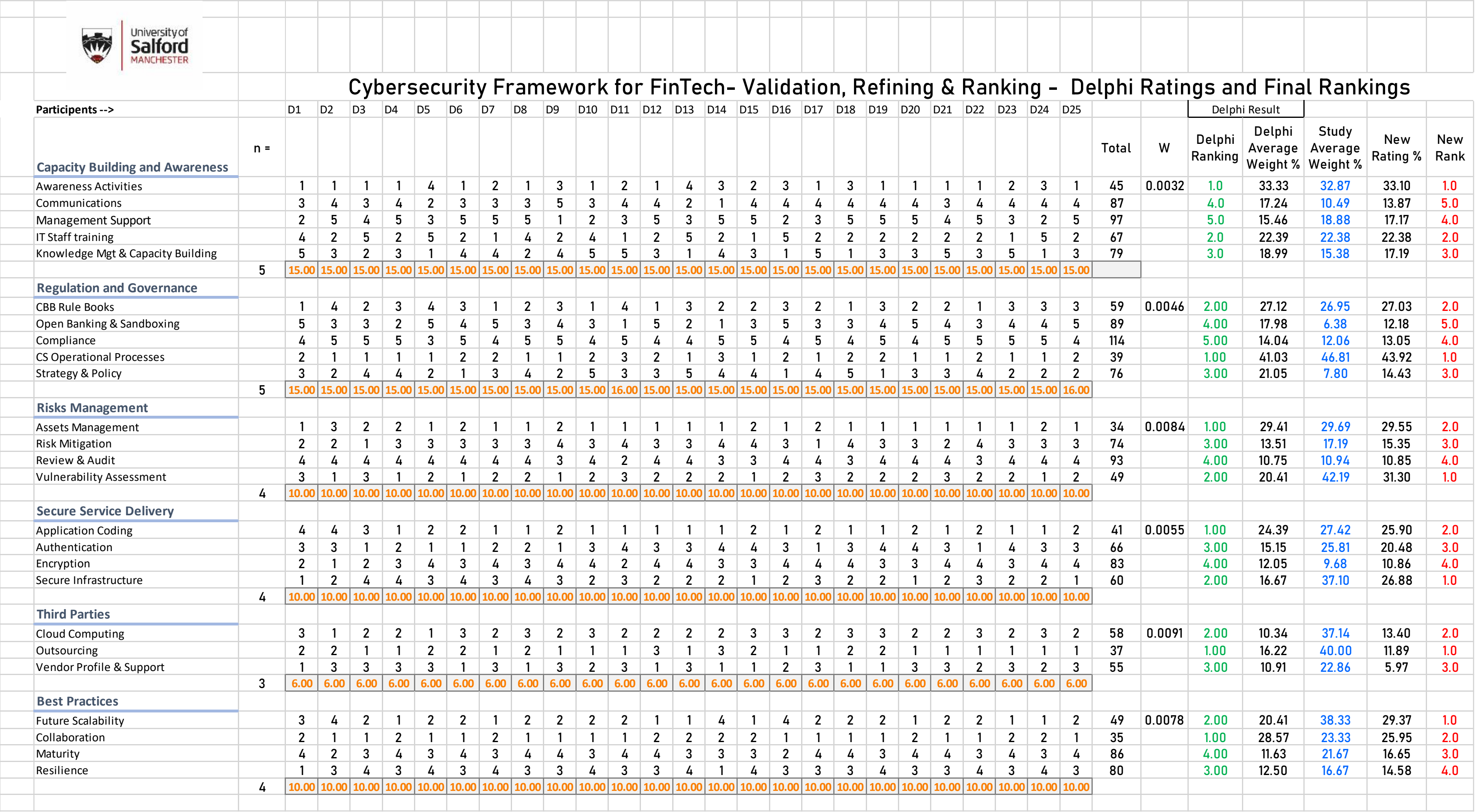
	Delphi Round 1	**Delphi Round 2**
N	25	25
Kendall's W	0.336	0.592
Chi-Square	41.960	73.970
df	5	5
Asymp. Sig.	0.000	0.000

5.5.7. Delphi Session – Part 2

Round 2's task for the participants was to rank the framework's controls by giving them a Likert scale rating and giving them the proper weights (on the scale of percentages). To measure the extent of consensus among the participants and so make use of Kendall's W coefficient concordance (W), the Likert scale ranking method was used (Schmidt, 1997).

For each control, fresh ratings and rankings were computed (Table 5.12) using the provided weights and statistical aggregate. The average ranking each control received from the Delphi participants is shown in the second column of Table 5.13, while the average percentage weights are displayed in the third column. The average weights provided by the findings of the primary data (interviews with participants) are shown in the fourth column, while the new average ratings from columns 3 and 4 are displayed in the fifth column. As a result, new rankings were created based on the ratings in column 5, as shown in the sixth column.

Table 5.12 Delphi Ratings and Final Ranking



Cybersecurity Framework for FinTech- Validation, Refining & Ranking - Delphi Ratings and Final Rankings

Participants -->		D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18	D19	D20	D21	D22	D23	D24	D25			Delphi Result				
Capacity Building and Awareness	n =																										Total	W	Delphi Ranking	Delphi Average Weight %	Study Average Weight %	New Rating %	New Rank
Awareness Activities		1	1	1	1	4	1	2	1	3	1	2	1	4	3	2	3	1	3	1	1	1	1	2	3	1	45	0.0032	1.0	33.33	32.87	33.10	1.0
Communications		3	4	3	4	2	3	3	3	5	3	4	4	2	1	4	4	4	4	4	4	3	4	4	4	4	87		4.0	17.24	10.49	13.87	5.0
Management Support		2	5	4	5	3	5	5	5	1	2	3	5	3	5	5	2	3	5	5	5	4	5	3	2	5	97		5.0	15.46	18.88	17.17	4.0
IT Staff training		4	2	5	2	5	2	1	4	2	4	1	2	5	2	1	5	2	2	2	2	2	2	1	5	2	67		2.0	22.39	22.38	22.38	2.0
Knowledge Mgt & Capacity Building		5	3	2	3	1	4	4	2	4	5	5	3	1	4	3	1	5	1	3	3	5	3	5	1	3	79		3.0	18.99	15.38	17.19	3.0
	5	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00							
Regulation and Governance																																	
CBB Rule Books		1	4	2	3	4	3	1	2	3	1	4	1	3	2	2	3	2	1	3	2	2	1	3	3	3	59	0.0046	2.00	27.12	26.95	27.03	2.0
Open Banking & Sandboxing		5	3	3	2	5	4	5	3	4	3	1	5	2	1	3	5	3	3	4	5	4	3	4	4	5	89		4.00	17.98	6.38	12.18	5.0
Compliance		4	5	5	5	3	5	4	5	5	4	5	4	4	5	5	4	5	4	5	4	5	5	5	5	4	114		5.00	14.04	12.06	13.05	4.0
CS Operational Processes		2	1	1	1	1	2	2	1	1	2	3	2	1	3	1	2	1	2	2	1	1	2	1	1	2	39		1.00	41.03	46.81	43.92	1.0
Strategy & Policy		3	2	4	4	2	1	3	4	2	5	3	3	5	4	4	1	4	5	1	3	3	4	2	2	2	76		3.00	21.05	7.80	14.43	3.0
	5	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	16.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	15.00	16.00							
Risks Management																																	
Assets Management		1	3	2	2	1	2	1	1	2	1	1	1	1	1	2	1	2	1	1	1	1	1	1	2	1	34	0.0084	1.00	29.41	29.69	29.55	2.0
Risk Mitigation		2	2	1	3	3	3	3	3	4	3	4	3	3	4	4	3	1	4	3	3	2	4	3	3	3	74		3.00	13.51	17.19	15.35	3.0
Review & Audit		4	4	4	4	4	4	4	4	3	4	2	4	4	3	3	4	4	3	4	4	4	3	4	4	4	93		4.00	10.75	10.94	10.85	4.0
Vulnerability Assessment		3	1	3	1	2	1	2	2	1	2	3	2	2	2	1	2	3	2	2	2	3	2	2	1	2	49		2.00	20.41	42.19	31.30	1.0
	4	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00							
Secure Service Delivery																																	
Application Coding		4	4	3	1	2	2	1	1	2	1	1	1	1	1	2	1	2	1	1	2	1	2	1	1	2	41	0.0055	1.00	24.39	27.42	25.90	2.0
Authentication		3	3	1	2	1	1	2	2	1	3	4	3	3	4	4	3	1	3	4	4	3	1	4	3	3	66		3.00	15.15	25.81	20.48	3.0
Encryption		2	1	2	3	4	3	4	3	4	4	2	4	4	3	3	4	4	4	3	3	4	4	3	4	4	83		4.00	12.05	9.68	10.86	4.0
Secure Infrastructure		1	2	4	4	3	4	3	4	3	2	3	2	2	2	1	2	3	2	2	1	2	3	2	2	1	60		2.00	16.67	37.10	26.88	1.0
	4	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00							
Third Parties																																	
Cloud Computing		3	1	2	2	1	3	2	3	2	3	2	2	2	2	3	3	2	3	3	2	2	3	2	3	2	58	0.0091	2.00	10.34	37.14	13.40	2.0
Outsourcing		2	2	1	1	2	2	1	2	1	1	1	3	1	3	2	1	1	2	2	1	1	1	1	1	1	37		1.00	16.22	40.00	11.89	1.0
Vendor Profile & Support		1	3	3	3	3	1	3	1	3	2	3	1	3	1	1	2	3	1	1	3	3	2	3	2	3	55		3.00	10.91	22.86	5.97	3.0
	3	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00	6.00							
Best Practices																																	
Future Scalability		3	4	2	1	2	2	1	2	2	2	2	1	1	4	1	4	2	2	2	1	2	2	1	1	2	49	0.0078	2.00	20.41	38.33	29.37	1.0
Collaboration		2	1	1	2	1	1	2	1	1	1	1	2	2	2	2	1	1	1	1	2	1	1	2	2	1	35		1.00	28.57	23.33	25.95	2.0
Maturity		4	2	3	4	3	4	3	4	4	3	4	4	3	3	3	2	4	4	3	4	4	3	4	3	4	86		4.00	11.63	21.67	16.65	3.0
Resilience		1	3	4	3	4	3	4	3	3	4	3	3	4	1	4	3	3	3	4	3	3	4	3	4	3	80		3.00	12.50	16.67	14.58	4.0
	4	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00	10.00							

Table 5.13 Delphi Ratings and Ranking

Capacity Building and Awareness	W	Delphi Average Ranking	Delphi Average Weight %	Study Average Weight %	New Weight %	New Rank
Awareness Activities	0.0032	1.0	33.33	32.87	33.10	1.0
Communications		4.0	17.24	10.49	13.87	5.0
Management Support		5.0	15.46	18.88	17.17	4.0
IT Staff training		2.0	22.39	22.38	22.38	2.0
Knowledge Management & Capacity Building		3.0	18.99	15.38	17.19	3.0
Regulation and Governance						
CBB Rule Books	0.0046	2.00	27.12	26.95	27.03	2.0
Open Banking & Sandboxing		4.00	17.98	6.38	12.18	5.0
Compliance		5.00	14.04	12.06	13.05	4.0
CS Operational Processes		1.00	41.03	46.81	43.92	1.0
Strategy & Policy		3.00	21.05	7.80	14.43	3.0
Risks Management						
Assets Management	0.0084	1.00	29.41	29.69	29.55	2.0
Risk Mitigation		3.00	13.51	17.19	15.35	3.0
Review & Audit		4.00	10.75	10.94	10.85	4.0
Vulnerability Assessment		2.00	20.41	42.19	31.30	1.0
Secure Service Delivery						
Application Coding	0.0055	1.00	24.39	27.42	25.90	2.0
Authentication		3.00	15.15	25.81	20.48	3.0
Encryption		4.00	12.05	9.68	10.86	4.0
Secure Infrastructure		2.00	16.67	37.10	26.88	1.0
Third Parties						
Cloud Computing	0.0091	2.00	10.34	37.14	13.40	2.0
Outsourcing		1.00	16.22	40.00	11.89	1.0
Vendor Profile & Support		3.00	10.91	22.86	5.97	3.0
Best Practices						
Future Scalability	0.0078	2.00	20.41	38.33	29.37	1.0
Collaboration		1.00	28.57	23.33	25.95	2.0
Maturity		4.00	11.63	21.67	16.65	3.0
Resilience		3.00	12.50	16.67	14.58	4.0

The rankings of the five controls of the framework's first principle – "Capacity Building and Awareness", show no change except for "Management Support" and "Communications" from 5th position to fourth place based on the new weights (or ratings). Again, with the second principle, "Regulation and Governance", a slight swap from 5th to 4th positions of the controls "Open Banking & Sandboxing" and "Compliance". However, controls ranking for the third principle, "Risks Management", shows total change as shown in Table 5.13.

In the same way, the controls ranking of the fourth principle, "Secure Service Delivery", remains unchanged except for the "Application Coding" and "Secure Infrastructure" controls. Controls of the fifth principle, "Third Parties", show no change at all. Finally, the "Best Practices" controls had some major adjustments in their rankings. As a result, Table 5.13 presents the final verified, improved, and ranked cybersecurity framework controls.

5.5.8. Validation and the Degree of Consensus

As discussed in Chapter 3, Kendall's coefficient of concordance (W) is used to quantify the level of agreement among participants of Delphi sessions based on rank correlation (Schmidt, 1997). Kendall's W is a measure of agreement that ranges from 0 to 1. A score of 0 indicates no agreement, while a score of 1 indicates total agreement, as shown in Table 3.6.

Thus, the degree of consensus (W) values shown in the second column of Table 5.14 for each set of controls (Principles) of 0.32, 0.46, 0.84, 0.55, 0..91, and 0.78 suggested an excellent agreement amongst the participants on the framework's controls rankings, according to (Schmidt, 1997) interpretation of Kendall's W coefficient.

Table 5.14 The degree of consensus (W) values

No	Principles	W
1	Capacity Building and Awareness	0.3208
2	Regulation and Governance	0.4574
3	Risks Management	0.8379
4	Secure Service Delivery	0.5546
5	Third Parties	0.9086
6	Best Practices	0.7832

Figure 5.7 demonstrates the degree of consensus based on the values listed in Table 5.14.

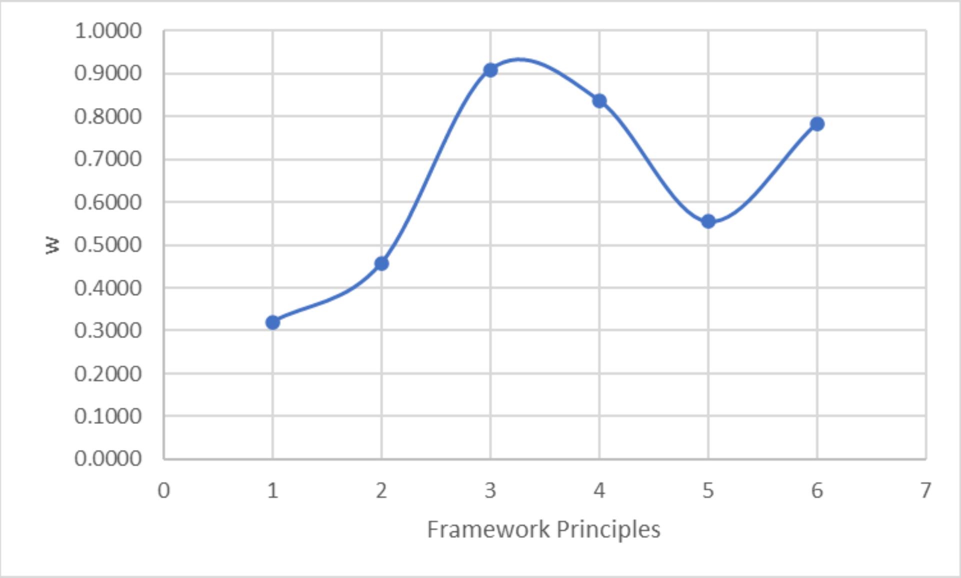


Figure 5.7 The degree of consensus (W) values.

Therefore, the findings of Kendall's W coefficient showed a high level of agreement among the participants, giving confidence in the outcomes and offering a valid justification to refine the framework as per their suggestions and comments.

5.6. Discussions, Recommendations and Suggestions

The NGN majlis’s panel speakers show excellent engagement with the research topic. Their feedback was critical for the framework's open and transparent validation and revising process. This phase will build on top of prior work and findings.

Various panellists discussed how they could utilise the framework to offer status reports to their upper management on addressing cybersecurity objectives, as well as the framework's usefulness in performing their tasks. The attendees in the panel discussions cited some of the unique needs of small and medium FinTech companies while providing thoughts on how to get them to begin establishing a cybersecurity plan. One participant mentioned that any FinTech innovation, regardless of its size, may make use of the framework by prioritising different parts of it and adding in new roles and duties as needed to achieve its goals.

The panel discussed how they can adapt the framework to fit various assessment requirements by combining it with different risk management tools and maturity models. In accordance with FinTech’s objectives, measurement and assessment relating to the framework had varied interpretations and implementation approaches. However, the framework can be easily used to detect operational cybersecurity patterns and to share expectations about the present cybersecurity posture with nontechnical stakeholders. Panellists stated that the framework’s flexibility and risk-based structure are helpful in creating unique and customised ways to evaluate and assess cyber risks.

The remining part of this section presents in a structured manner the key themes that emerged from the NGN majlis workshop discussions and highlights the main recommendations by panellists and participants. It is essential to understand the implications of the experts’ discussions and how they relate to the framework enhancements, suggestions, and recommendations.

5.6.1. The Framework is Useful for FinTech Businesses of All Sizes.

FinTech’s stakeholders in Bahrain will put in further effort to ensure that the framework is beneficial to FinTech of all sizes in addressing cybersecurity threats.

5.6.2. National Collaboration

By giving priority to interactions with government, regulators, and the financial sector, it will facilitate and promote national cooperation and involvement. In this manner, the framework will be regarded as a national resource for cybersecurity controls tailored for FinTech innovations in Bahrain.

5.6.3. Framework High-Level Detail

The panellists made it clear that the framework's main characteristics, such as its flexibility, simplicity, and ease of use, will help FinTech of all sizes use it. To guarantee that the framework is scalable and adaptable for a variety of FinTech, it should retain the current level of details and remain as a framework, offering context and links to international standards but not replacing them. Panellists argue that while some might benefit from simple and basic interpretations of the framework's basic components, others might demand more in-depth details, such as links and mappings to particular cybersecurity standards.

5.6.4. Informative References

One panellist proposed the usefulness of having informative references and voiced interest in providing additional mappings to the recognised and widely acknowledged cybersecurity standards in order to provide FinTech businesses further implementation guidance. While the idea of informative references was generally accepted, the researcher addressed this in section 6.3 of the thesis’s last chapter.

5.6.5. Vendor and Technology Neutral

A panellist argues that maintaining technology neutrality is a crucial aspect of the proposed cybersecurity framework. As the technological landscape continues to undergo rapid changes, it is essential for the framework to address specific issues, developments, and applications in cybersecurity updates. However, it is equally important to ensure that these updates do not compromise the framework's ability to be effectively applied in its intended context. He emphasised “The need to accommodate FinTech organisations, irrespective of the technology or services they employ, while incorporating changes in cybersecurity practices. This approach will enable the framework to remain adaptable and inclusive, catering to the evolving needs of FinTech stakeholders while preserving its technology neutrality”.

5.6.6. Cybersecurity Measurements and Assessments

A participant asks the panel for further guidance and materials to enable measurements and assessments of the FinTech use of the framework and to clearly describe how the framework may support the measurement and assessment of cybersecurity activities.

Regardless of the underlying risk management approach, FinTech innovations have a shared taxonomy and terminology to convey the results of their assessment activities. This fact is confirmed by one panellist as he stated that “finding out how successfully an organisation is managing cybersecurity risk, as well as if and how they are making improvements, is a key objective of cybersecurity measurement and assessment. From system-level to organizational-wide, the activities that enable measurement and evaluation serve as inputs for figuring out maturity and supporting risk management choices”. He added that “because each FinTech Firm has different risks, goals, and systems, different approaches are used to attain the aims outlined in the framework principles. As a result, the context influences how results are measured and assessed. In order to maintain flexibility in how FinTech may apply the framework, it is not advisable to have a single strategy of the assessment in the framework”. Therefore, FinTech might use the framework in conjunction with risk management techniques and maturity models to address queries regarding the effectiveness of their cybersecurity activities.

5.7. Delphi Survey Notes

Notes captured from the Delphi questionnaire provide suggestions for its improvement and implementation. The recommendations are generally valid and provide valuable insights into the potential areas for improvement in the framework. However, the D1 suggests having a critical evaluation of the framework after adopting it to assess its effectiveness in improving cybersecurity for FinTech in Bahrain. Furthermore, D2 argued that the framework is too broad and lacks specificity, making it difficult for small FinTech to implement it effectively. D3 pointed out that the framework is voluntary, which may limit its effectiveness in improving cybersecurity across all FinTech innovations. Additionally, D4 suggests addressing the challenges that FinTech may face in implementing the framework, such as the need for specialised cybersecurity expertise and costs associated with the implementation process.

5.8. Summary

The review of the literature, the qualitative research approach, and interviewing experts facilitated the development of the cybersecurity framework for FinTech in Bahrain. One approach to getting feedback from stakeholders on the framework's use today and how it could evolve to address FinTech's future cybersecurity challenges was via a panel discussion. The panel or a workshop is an excellent venue for engagement with FinTech’s stakeholders.

Using two Delphi rounds with 25 experts working at various banking and FinTech businesses and at different operational levels, the framework’s components were reviewed, validated, refined, and ranked. This effort not only led to the enhancement of the framework but also refined the controls with the objective of making the framework more straightforward for implementation and more usable for different sizes of FinTech Innovations.

In addition to offering cybersecurity and FinTech stakeholders a common language, the framework is acknowledged as being a fundamental baseline to securing FinTech businesses. This is in large part due to the researchers' dedication to observing meaningful stakeholders’ feedback, which resulted in widespread community acceptance during the early stages of the framework's development. Furthermore, the findings of Kendall's W coefficient shown in Table 5.14 and Figure 5.7 confirm a high level of agreement among the participants, giving confidence in the outcomes and offering a valid justification to refine the framework as per their suggestions and comments.

This page intentionally left blank

Chapter 6: Discussion and Recommendations

6. Chapter 6: Discussion and Recommendations

6.1. Introduction

From the literature, Bahrain has embraced Vision 2030 as a strategic plan to drive economic expansion and foster the progress of the country. The vision articulated the kingdom's broad objectives and aspirations to establish itself as a globally recognised model of a successful and innovative nation. The kingdom seeks to establish an attractive environment for technological innovations in finance, with a strong emphasis on the broad integration of FinTech as a vital facilitator (BFB, 2022).

This study proposed a cybersecurity framework for FinTech that establishes fundamental principles to be implemented by all FinTech firms in the kingdom. The purpose was to mitigate the cybersecurity risks that arise from the extensive use of FinTech innovations.

The research used a qualitative method to gather and synthesise scientific community-proposed cybersecurity frameworks for FinTech and to determine the research gap in Bahrain. It answered the research question by highlighting the cyber threats facing FinTech sector. From the literature, there were several countermeasures to address these challenges. Regulatory guidelines and existing cybersecurity standards were some instruments to establish a cybersecurity baseline at FinTech companies.

The study encouraged cross-pollination among research methodologies and provided suggestions for prospective cybersecurity framework for FinTech businesses in Bahrain. It highlighted the critical aspects involved in developing a cybersecurity framework for FinTech, specifically for Bahrain. Analysing the in-depth interviews of executives and FinTech business owners, led to a proposed cybersecurity framework that incorporates key factors that were not addressed with the national cybersecurity guidelines.

The CFFB sought to aid these firms in establishing appropriate cybersecurity governance and a strong infrastructure, as well as essential analytical and preventative measures. The CFFB can help to identify relevant controls and offers advice on how to gauge maturity. The framework's adoption and implementation are critical steps in securing Bahrain’s FinTech institutes and addressing cybersecurity threats. This will guarantee that cybersecurity risks are effectively addressed and well managed. The optimal goal is to raise the level of cybersecurity and create a trusted electronic environment for both the customers and FinTech companies in Bahrain.

6.2. The Proposed CFFB

Developing the CFFB involves detailed analysis of several areas to guarantee the security and reliability of FinTech systems. The framework consists of the following elements:

- Six Main Principles
- 25 Controls
- 50 Guidelines

As discussed in Chapter 5 and after validating CFFB through experts review and Delphi sessions, the revised and final visual representation of the framework is shown in Figure 6.1

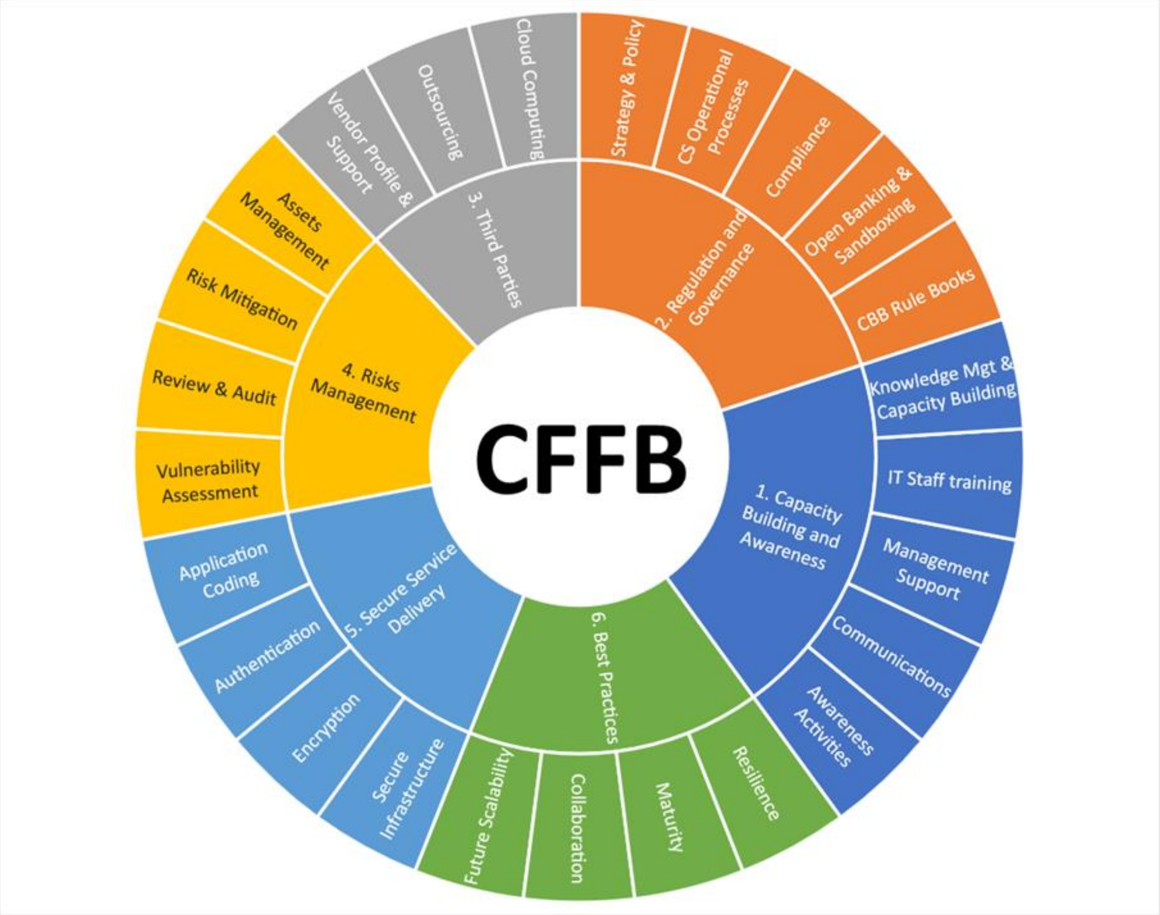


Figure 6.1 The Principles and Controls of the Proposed CFFB.

Table 6.1 lists a comprehensive CFFB's main principles and its controls.

Table 6.1 CFFB Framework's Principles and Controls

Principle	Controls	
1. Capacity Building and Awareness	1.1 Awareness Activities 1.2 Communications 1.3 Management Support	1.4 IT Staff Training 1.5 Knowledge Mgt & Capacity Building
2. Regulation and Governance	2.1 CBB Rule Books 2.2 Open Banking & Sandboxing 2.3 Compliance	2.4 Operational Processes 2.5 Strategy & Policy
3. Third Parties	3.1 Cloud Computing 3.2 Outsourcing	3.3 Vendor Profile & Support
4. Risk Management	4.1 Assets Management 4.2 Risk Mitigation	4.3 Review & Audit 4.4 Vulnerability Assessment
5. Secure Service Delivery	5.1 Application Coding 5.2 Authentication	5.3 Encryption 5.4 Secure Infrastructure
6. Best Practices	6.1 Future Scalability 6.2 Collaboration	6.3 Maturity 6.4 Resilience

In the following subsections, we will discuss the CFFB's main components and elements in details.

6.2.1. Capacity Building and Awareness

Raising cybersecurity awareness among stakeholders is crucial for the success of any cybersecurity framework. This involves educating employees, customers, and relevant parties about cybersecurity risks, best practices, and potential threats specific to the FinTech sector. Awareness activities can include training sessions, workshops, seminars, and awareness campaigns. These initiatives should emphasise the importance of cybersecurity, promote a culture of security, and encourage reporting of any suspicious activities.

Moreover, research participants indicated that building a highly skilled and knowledgeable IT workforce is essential for effective cybersecurity management in FinTech. IT staff training should cover a wide range of topics, including secure coding practices, network security, incident response, data protection, and compliance with relevant regulations. Continuous training programs should be provided to keep IT staff updated with the latest cybersecurity threats, vulnerabilities, and mitigation techniques. Training should also focus on developing skills in threat intelligence, risk assessment, and secure system design.

Based on the research analysis, knowledge management plays a vital role in establishing and maintaining a robust cybersecurity framework. It involves capturing, organising, and sharing cybersecurity-related knowledge, best practices, and lessons learned. This can be achieved through the implementation of knowledge management systems, incident reporting mechanisms, and collaboration platforms. By effectively managing knowledge, organisations can enhance their incident response capabilities, improve decision-making processes, and foster a culture of continuous improvement in cybersecurity.

Furthermore, experts who participated in this study highlight that capacity-building initiatives can include establishing cybersecurity centres of excellence, promoting research and development in cybersecurity, fostering collaboration between industry and academia, and encouraging innovation in cybersecurity solutions. Capacity-building efforts should focus on strengthening the technical skills of cybersecurity professionals, promoting information sharing and cooperation among stakeholders, and enhancing the overall cybersecurity posture of the FinTech ecosystem. Table 6.2 lists all the controls and guidelines for the Capacity Building and Awareness Principle.

Table 6.2 Controls and Guidelines for Capacity Building and Awareness Principle.

1	**Capacity Building and Awareness**	
1.1	**Awareness Activities**	
Description	*They involve disseminating information, materials, and resources to educate stakeholders about various aspects of the FinTech industry, such as Cyber threats, protection measures, regulatory changes, emerging risks, and best practices.*	
	Guidelines	
1.1.1	Awareness activities can include training sessions, workshops, seminars, and awareness campaigns. These activities should suit the local culture of people in Bahrain when it comes to social engineering tricks and the treatment of personal data.	

1.1.2	Emphasise the importance of cybersecurity, promote a culture of security, and encourage reporting of any suspicious activities.	
1.2	**Communications**	
Description	*Communications help to raise awareness by using various channels and formats, such as publications, webinars, podcasts, social media, events and campaigns. Communication can foster dialogue, collaboration and learning among diverse actors and audiences.*	
	Guidelines	
1.2.1	Ensure that employees, management, and other relevant parties recognise their responsibilities and roles in maintaining cybersecurity. This includes promoting awareness of security best practices, providing regular updates on emerging threats and vulnerabilities, and establishing communication channels for reporting security incidents.	
1.2.2	Encourage communication and information sharing with external parties, for instance, regulatory bodies, law enforcement entities, and business peers, to stay informed about the latest cybersecurity trends and collaborate on incident response.	
1.3	**Management Support**	
Description	*The commitment and involvement of senior managers and decision-makers in providing the necessary resources, guidance and incentives for the development of skills and knowledge among their staff and stakeholders. It entails creating a conducive environment for learning, innovation, and collaboration and fostering a culture of continuous improvement and accountability.*	
	Guidelines	
1.3.1	Allocate adequate resources, budget, and personnel to implement and maintain effective cybersecurity measures.	
1.3.2	Establishing a mindset of cybersecurity awareness across the FinTech company by promoting employee training and fostering a proactive approach to risk management. Ensure cybersecurity receives the necessary attention and resources to protect the FinTech ecosystem.	
1.4	**IT Staff training**	

Description	*IT staff training is an integral part of Capacity Building and Awareness efforts, particularly in the technology-driven FinTech industry.*	
	Guidelines	
1.4.1	Cover a broad spectrum of subjects, namely secure coding practices, network security, incident response, data protection, and compliance with relevant regulations.	
1.4.2	Provide continuous training programs to keep IT staff updated with the latest cybersecurity threats, vulnerabilities, and mitigation techniques. Training should also focus on developing skills in threat intelligence, risk assessment, and secure system design.	
1.5	**Knowledge Management & Capacity Building**	
Description	*Knowledge management involves the systematic collection, organisation, and dissemination of information, best practices, and lessons learned within the FinTech industry. Capacity building focuses on developing the skills, competencies, and capabilities of individuals and organisations to effectively apply knowledge and address industry challenges.*	
	Guidelines	
1.5.1	Capturing, organising, and sharing cybersecurity-related knowledge, best practices, and lessons learned.	
1.5.2	Implementation of knowledge management systems, incident reporting mechanisms, and collaboration platforms.	

6.2.2. Regulation and Governance

Regulation and governance are critical for establishing a robust cybersecurity framework. Bahrain has made significant progress in this regard by implementing cybersecurity regulations specific to the financial sector. The CBB has established guidelines to ensure cybersecurity compliance and risk management. These regulations outline the responsibilities of financial institutions, set minimum security requirements, and define reporting mechanisms for cybersecurity incidents.

The literature disclosed that the CBB has issued rulebook that provided detailed guidelines and requirements for financial institutions operating in Bahrain. This rulebook covered various areas, including cybersecurity. They outline the standards expected from financial institutions in terms of risk management, data protection, incident response, and business continuity planning. Adhering to this rulebook is crucial for FinTech companies to ensure compliance with cybersecurity regulations.

In addition, the open banking project encourages the safe exchange of financial information across various financial organisations, including traditional banks and FinTech companies. In the context of cybersecurity, open banking introduces new challenges and risks that need to be considered. During the Delphi discussion, participants emphasised that the framework should consider the implementation of strong authentication mechanisms, robust access controls, encryption of data at rest and in transit, and regular security assessments to ensure the integrity and confidentiality of customer data in open banking environments.

According to the research participants, FinTech sandboxing plays a crucial role in cybersecurity by allowing new FinTech startups to identify and mitigate vulnerabilities before deploying them in a live environment. The framework should encourage the use of sandboxes for testing and validating security measures, ensuring that FinTech innovations meet the necessary security standards.

The research analysis recommends that the framework should consider mechanisms to assure compliance with appropriate cybersecurity regulations, such as Bahrain’s data protection laws and financial-specific standards. Regular audits, assessments, and penetration testing are conducted to detect and rectify any compliance shortfalls. Additionally, FinTech should establish processes for monitoring changes in regulations and updating their cybersecurity practices accordingly.

Moreover, operational processes encompass the day-to-day activities of FinTech innovations. These processes should be designed with cybersecurity in mind, incorporating security controls and best practices. This includes secure software development practices, secure configuration management, access control mechanisms, vulnerability management, and incident response procedures. The framework provides guidelines and standards for operational processes to ensure consistent and effective security practices throughout the FinTech organisation.

Finally, formulating a comprehensive cybersecurity strategy and policy is a crucial component of the cybersecurity framework. The strategy should align with the FinTech's overall goals, risk appetite, and regulatory requirements. It should define the objectives, priorities, and resource allocation for cybersecurity initiatives. The policy, on the other hand, provides specific guidelines and requirements for cybersecurity practices, including access controls, data protection, incident response, and employee awareness. A well-defined strategy and policy help FinTech businesses establish a proactive and risk-based approach to cybersecurity. Table 6.3 lists all the controls and guidelines for the Regulation and Governance Principle.

Table 6.3 Controls and Guidelines for Regulation and Governance Principle.

2	**Regulation and Governance**	
2.1	**CBB Rule Books**	
Description	*CBB Rule Books are regulatory frameworks created and enforced by central banks or regulatory authorities. These rule books establish specific requirements and guidelines for the FinTech industry to ensure the security and integrity of operations.*	
	Guidelines	
2.1.1	Outline the standards expected from FinTech institutions in terms of risk management, data protection, incident response, and business continuity planning.	
2.1.2	Adhering to these rule books is crucial for FinTech companies to ensure compliance with cybersecurity regulations.	
2.2	**Open Banking & Sandboxing**	
Description	*Open Banking involves securely exchanging client financial data between financial institutions and authorised third-party providers with the customer's consent. It aims to foster innovation, competition, and better customer experiences in the financial industry.* *Sandboxing, on the other hand, involves creating isolated environments for testing and validating new technologies and applications without posing a risk to the production environment.*	
	Guidelines	
2.2.1	Implement strong authentication mechanisms, robust access controls, encryption of data at rest and in transit, and regular security assessments to ensure the integrity and confidentiality of customer data in open banking environments.	

2.2.2	Encourage the use of sandboxes for testing and validating security measures, ensuring that FinTech innovations meet the necessary security standards.	
2.3	**Compliance**	
Description	*Compliance refers to adhering to applicable laws, regulations, and industry standards regarding cybersecurity in the FinTech sector. Regulatory frameworks set requirements for data protection, security controls, incident reporting, and customer protection.*	
	Guidelines	
2.3.1	Ensure compliance with relevant cybersecurity regulations, such as data protection laws and industry-specific standards.	
2.3.2	Regular audits, assessments, and penetration testing are conducted to detect and rectify any compliance shortfalls.	
2.4	**CS Operational Processes**	
Description	*Cybersecurity operational processes encompass the day-to-day activities and procedures involved in managing and protecting FinTech's information systems and data. These processes include vulnerability management, incident response, access control, and network monitoring,*	
	Guidelines	
2.4.1	Includes secure software development practices, secure configuration management, access control mechanisms, vulnerability management, and incident response procedures.	
2.4.2	Provide guidelines and standards for operational processes to ensure consistent and effective security practices throughout the organisation.	
2.5	**Strategy & Policy**	
Description	*Cybersecurity strategy and policies provide a plan for managing and mitigating cybersecurity risks within FinTech firms. The strategy outlines FinTech's long-term goals, risk appetite, and strategic initiatives to protect its systems and data. Policies, on the other hand, define specific guidelines, procedures, and controls that employees must follow to ensure compliance and protect against cyber threats.*	

	Guidelines	
2.5.1	Align the strategy with FinTech's overall goals, risk appetite, and regulatory requirements. It should define the objectives, priorities, and resource allocation for cybersecurity initiatives.	
2.5.2	The policy provides specific guidelines and requirements for cybersecurity practices, including access controls, data protection, incident response, and employee awareness.	

6.2.3. Third Parties

Third-party relationships are common in the FinTech industry, and they can introduce cybersecurity risks if not managed effectively. The framework should address the risks associated with third-party vendors, including data breaches, unauthorised access, and supply chain attacks. It should include guidelines for conducting due diligence on third-party vendors, assessing their cybersecurity capabilities, and establishing contractual agreements that outline security requirements. The framework should also emphasise ongoing monitoring of third-party activities and periodic security assessments to ensure compliance with cybersecurity standards.

Another common area for FinTech is its heavy reliance on cloud computing. FinTech can enjoy various advantages through its use, which include scalability, flexibility, and cost-effectiveness. However, it also introduces unique cybersecurity considerations. The cybersecurity framework should provide guidelines for securely adopting and managing cloud services. This includes ensuring the selection of reputable Cloud Service Providers (CSPs) with robust security measures, implementing strong access controls and encryption for data stored in the cloud, and monitoring for unauthorised access or data exposure. The framework should also address data sovereignty and compliance with applicable data protection regulations when utilising cloud services.

Outsourcing certain functions or services is common in the FinTech sector. However, it brings cybersecurity risks, such as loss of control over sensitive data or inadequate security practices by the outsourced party. The framework should include guidelines for evaluating the cybersecurity capabilities of outsourced providers, including conducting due diligence, defining security requirements in contracts, and monitoring the outsourced activities. It should also address incident response and data breach notification procedures to ensure timely and appropriate actions in case of a security incident involving the outsourced party.

The support provided by vendors played a significant role in the overall cybersecurity posture of FinTech companies. The framework should emphasise the importance of evaluating vendor profiles in terms of their security practices, track record, and compliance with relevant standards. It should include guidelines for assessing the vendor's ability to provide ongoing support, including timely security updates, vulnerability management, and incident response support. Additionally, the framework should outline procedures for monitoring the vendor's security posture and taking appropriate actions in case of security breaches or non-compliance. Table 6.4 lists all the controls and guidelines for the Third Parties Principle.

Table 6.4 Controls and Guidelines for Third Parties Principle.

3	**Third Parties**	
3.1	**Cloud Computing**	
Description	*Cloud computing uses distant servers on the Internet for storing, managing, and processing data rather than depending on local servers or desktop systems.*	
	Guidelines	
3.1.1	Ensure the selection of reputable Cloud Service Providers (CSPs) with robust security measures, implementing strong access controls and encryption for data stored in the cloud, and monitoring for unauthorised access or data exposure.	
3.1.2	Address data sovereignty and compliance with applicable data protection regulations when utilising cloud services.	
3.2	**Outsourcing**	
Description	*Outsourcing is the practice of assigning specific corporate operations or responsibilities to external third-party suppliers or service providers.*	
3.2.1	**Guidelines**	
3.2.2	Evaluate the cybersecurity capabilities of outsourced providers, including conducting due diligence, defining security requirements in contracts, and monitoring the outsourced activities.	

	Address incident response and data breach notification procedures to ensure timely and appropriate actions in case of a security incident involving the outsourced party.	
3.3	**Vendor Profile & Support**	
Description	*Vendor profile and support refer to the assessment and management of third-party vendors in terms of their cybersecurity capabilities and support.*	
	Guidelines	
3.3.1	Emphasise the importance of evaluating vendor profiles in terms of their security practices, track record, and compliance with relevant standards. It should include guidelines for assessing the vendor's ability to provide ongoing support, including timely security updates, vulnerability management, and incident response support.	
3.3.2	Outline procedures for monitoring the vendor's security posture and taking appropriate actions in case of security breaches or non-compliance.	

6.2.4. Risks Management

Risk management is an essential aspect of FinTech's cybersecurity. It involves identifying, assessing, and prioritising cybersecurity risks to make informed decisions on risk mitigation strategies. The cybersecurity framework should include guidelines and processes for conducting risk assessments, establishing risk management guidelines, and defining risk tolerance levels. It should also outline procedures for monitoring and reviewing risks on an ongoing basis to ensure that appropriate controls are in place to mitigate identified risks effectively.

Additionally, effective management of assets is essential for cybersecurity in the FinTech industry. Assets include both physical and digital resources, such as hardware, software, data, and intellectual property. The framework should provide guidelines for asset inventory management, classification of assets based on their criticality, access controls, and data protection measures. It should also address procedures for secure disposal or decommissioning of assets to prevent potential data breaches or unauthorised access.

According to the research findings, the cybersecurity framework should outline specific risk mitigation strategies and best practices for FinTech firms. Risk mitigation involves implementing measures and controls to reduce the impact and likelihood of cybersecurity risks. This includes setting up security solutions in place, including firewalls, intrusion detection/prevention systems, access restrictions, and data encryption. The framework should also emphasise the need for regular security updates and patches, security awareness training, incident response planning, and business continuity controls to minimise the impact of possible cybersecurity incidents.

Furthermore, regular review and audit processes are critical for ensuring the effectiveness and compliance of cybersecurity measures. The framework should include guidelines for conducting internal and external reviews and audits of FinTechs' cybersecurity practices. This includes evaluating the implementation of security controls, assessing adherence to policies and procedures, and identifying areas for improvement. The framework should also define reporting mechanisms and outline actions to address identified gaps or deficiencies.

According to the participants' answers, the framework should emphasise the importance of conducting regular vulnerability assessments to identify potential weaknesses that could be exploited by attackers. This may involve using automated scanning tools, penetration testing, and code reviews to identify vulnerabilities in the IT infrastructure. The framework should also provide guidelines for prioritising and remediating identified vulnerabilities to minimise the risk of exploitation. Table 6.5 lists all the controls and guidelines for the Risks Management Principle.

Table 6.5 Controls and Guidelines for Risks Management Principle.

4	**Risks Management**	
4.1	**Assets Management**	
Description	*Assets management involves identifying, classifying, and understanding the critical assets and information systems within an organisation. In the context of cybersecurity, assets can include client data, financial records, infrastructure, and software applications.*	
	Guidelines	
4.1.1	Provide guidelines for asset inventory management, classification of assets based on their criticality, access controls, and data protection measures.	

4.1.2	Address procedures for secure disposal or decommissioning of assets to prevent potential data breaches or unauthorised access.	
4.2	**Risk Mitigation**	
Description	*Risk mitigation is the process of detecting, evaluating, and applying measures to reduce or eliminate potential risks.*	
	Guidelines	
4.2.1	Outline specific risk mitigation strategies and best practices for FinTech organisations. This may include implementing security solutions, for instance, firewalls, intrusion detection/prevention systems, data encryption, and access controls.	
4.2.2	Emphasise the need for regular security updates and patches, security awareness training, incident response planning, and business continuity measures to minimise the impact of potential cybersecurity incidents.	
4.3	**Review & Audit**	
Description	*Regular reviews and audits help evaluate the efficiency of current security measures, policies, and controls. They entail evaluating compliance with regulatory mandates and industry guidelines, and internal policies.*	
	Guidelines	
4.3.1	Conduct internal and external reviews and audits of FinTech organisations' cybersecurity practices. This includes evaluating the implementation of security controls, assessing adherence to policies and procedures, and identifying areas for improvement.	
4.3.2	Define reporting mechanisms and outline actions to address identified gaps or deficiencies.	
4.4	**Vulnerability Assessment**	
Description	*Vulnerability assessment is the process of identifying and evaluating vulnerabilities in FinTech systems, networks, and applications. It involves conducting comprehensive scans and tests to identify potential weaknesses that can be exploited by cyber threats.*	
	Guidelines	

4.4.1	Emphasise the importance of conducting regular vulnerability assessments to identify possible weaknesses that could be utilised by attackers. This may involve using automated scanning tools, penetration testing, and code reviews to recognise vulnerabilities in the IT infrastructure.	
4.4.2	Provide guidelines for prioritising and remediating identified vulnerabilities to minimise the risk of exploitation.	

6.2.5. Secure Service Delivery

Secure service delivery ensures that FinTech services are provided to customers in a secure and reliable manner. This involves implementing measures to protect against unauthorised access, data breaches, and service disruptions. Based on participant interviews, the framework should include guidelines for secure service delivery, such as implementing secure communication protocols, secure Application Programming Interface (API), robust access controls, and monitoring mechanisms to detect and respond to potential security incidents or service disruptions.

Another measure is that secure FinTech's application coding practices are essential to minimise vulnerabilities and prevent potential exploitation by attackers. The cybersecurity framework should emphasise the use of secure coding best practices, secure development methodologies, and regular code reviews to identify and fix security flaws. Additionally, it should promote incorporating security measures, including secure session management, verification of input, and output decoding throughout the software development cycle. Authentication is a critical aspect of cybersecurity in FinTech. It ensures that only authorised individuals can access systems, applications, and data. The framework should promote solid authentication techniques, such as Multi-Factor Authentication (MFA), biometrics, and secure password policies. It should also address secure storage and transmission of authentication credentials, protection against brute-force attacks, and secure user identity management practices.

Another factor to consider while maintaining a secure service delivery in FinTech innovations is encryption. It plays a vital role in protecting sensitive data in transit and at rest. Interviewees emphasise the use of encryption to safeguard data across various channels, including communication networks, storage systems, and databases. This includes implementing strong encryption algorithms, managing encryption keys securely, and ensuring the integrity and confidentiality of data during transmission and storage.

In general, a secure infrastructure forms the foundation of a robust cybersecurity measure. It involves implementing secure network architecture, firewalls, intrusion detection/prevention systems, and security monitoring tools. The framework should include guidelines for regular security assessments, vulnerability management, and patch management to address potential security weaknesses in the infrastructure. Additionally, secure infrastructure practices should cover physical security measures, such as access controls, monitoring, and disaster recovery plans. Table 6.6 lists all the controls and guidelines for the Secure Service Delivery Principle.

Table 6.6 Controls and Guidelines for Secure Service Delivery Principle.

5	**Secure Service Delivery**	
5.1	**Application Coding**	
Description	*Application coding refers to the process of writing and developing software applications.*	
	Guidelines	
5.1.1	Emphasise the use of secure coding standards, secure development methodologies, and regular code reviews to identify and fix security flaws.	
5.1.2	Encourage the integration of security controls, such as input validation, output encoding, and secure session management, into the software development lifecycle.	
5.2	**Authentication**	
Description	*Authentication is the verification of the identity of individuals or systems trying to gain entry to resources or services.*	
	Guidelines	
5.2.1	Promote solid authentication techniques, such as Multi-Factor Authentication (MFA), biometrics, and secure password policies.	
5.2.2	Address secure storage and transmission of authentication credentials, protection against brute-force attacks, and secure user identity management practices.	
5.3	**Encryption**	
Description	*Encryption involves converting data into an unreadable form using cryptographic techniques.*	

	Guidelines	
5.3.1	Emphasise the use of encryption to safeguard data across various channels, including communication networks, storage systems, and databases.	
5.3.2	Implement strong encryption algorithms, manage encryption keys securely, and ensure the integrity and confidentiality of data during transmission and storage.	
5.4	**Secure Infrastructure**	
Description	*Secure infrastructure encompasses the fundamental hardware, software, and network elements that facilitate the provision of FinTech services.*	
	Guidelines	
5.4.1	Implement secure network architecture, security monitoring tools, intrusion detection firewalls, and prevention systems.	
5.4.2	Conduct regular security assessments, vulnerability management, and patch management to address potential security weaknesses in the infrastructure. Additionally, secure infrastructure practices should cover physical security procedures, including access restrictions, monitoring, and disaster recovery plans.	

6.2.6. Best Practices

In developing a cybersecurity framework, it is crucial to incorporate industry best practices. It encompasses a set of guidelines, standards, and processes that are widely recognised as effective in mitigating cybersecurity risks. The cybersecurity framework should include these best practices, such as those established by international organisations like NIST, ISO, and PCI-DSS. It should cover areas such as risk management, secure coding, incident response, access controls, and employee awareness training. By incorporating best practices, the framework can ensure that FinTech organisations adopt proven security measures to defend their systems, data, and clients.

Moreover, the framework should be designed with future scalability in mind. The FinTech industry is rapidly evolving, and new technologies, services, and threats emerge over time. The framework should be flexible and adaptable to accommodate these changes. It should allow for the integration of new security controls, the adoption of emerging technologies, and the ability to address evolving risks. By considering future scalability, the framework can provide a long-term cybersecurity roadmap that remains effective even as the FinTech landscape evolves.

Additionally, collaboration is a key part of the implementation of a cybersecurity framework. It involves cooperation between different stakeholders, including government agencies, regulatory bodies, FinTech, and cybersecurity service providers. The framework should promote collaboration for sharing threat intelligence, exchanging best practices, and coordinating incident response activities. Collaboration can enhance the collective cybersecurity resilience of the FinTech sector in Bahrain by leveraging combined knowledge, resources, and expertise.

According to participants, a mature framework demonstrates that cybersecurity measures are well-defined, consistently applied, and continuously improved. It includes regular assessments, audits, and evaluations to identify gaps and areas for enhancement. A mature framework also promotes a culture of cybersecurity awareness and accountability among all stakeholders. It evolves as new threats and technologies emerge, ensuring that the cybersecurity posture of FinTech innovations in Bahrain remains solid and adaptive.

Finally, the cybersecurity framework should focus on building resilience by implementing measures that prevent, detect, respond to, and recover from security breaches. In this context, resilience refers to the ability of the FinTech to withstand and recover from cybersecurity incidents. This includes incident response planning, business continuity management, data backup and recovery procedures, and periodic testing and evaluation of these processes. By prioritising resilience, the framework ensures that FinTech organisations can quickly mitigate the effect of cybersecurity incidents and resume routine activities. Table 6.7 lists all the controls and guidelines for the Best Practices Principle.

Table 6.7 Controls and Guidelines for Best Practices Principle.

6	**Best Practices**	
6.1	**Future Scalability**	
Description	*Future scalability refers to the ability of a cybersecurity framework or practice to adapt and accommodate future growth and changes in the FinTech organisation.*	
	Guidelines	
6.1.1	Allow for the integration of new security controls, the adoption of emerging technologies, and the ability to address evolving risks.	
6.1.2	Provide a long-term cybersecurity roadmap that remains effective even as the FinTech landscape evolves.	
6.2	**Collaboration**	
Description	*Collaboration refers to the act of working together with internal stakeholders, industry peers, regulatory bodies, and other relevant entities to enhance cybersecurity in the FinTech sector.*	
	Guidelines	
6.2.1	Cooperation between different stakeholders, including government agencies, regulatory bodies, FinTech organisations, industry associations, and cybersecurity experts.	
6.2.2	Encourage collaboration for sharing threat intelligence, exchanging best practices, and coordinating incident response activities. Collaboration can enhance the collective cybersecurity resilience of the FinTech sector in Bahrain by leveraging combined knowledge, resources, and expertise.	
6.3	**Maturity**	
Description	*Maturity in the context of cybersecurity best practices for FinTech refers to the level of development and effectiveness of the FinTech security program.*	
	Guidelines	
6.3.1	Demonstrate that cybersecurity measures are well-defined, consistently applied, and continuously improved. It includes regular assessments, audits, and evaluations to identify gaps and areas for enhancement.	

6.3.2	Promote a culture of cybersecurity awareness and accountability among all stakeholders. It evolves as new threats and technologies emerge, ensuring that the cybersecurity posture of FinTech organisations in Bahrain remains solid and adaptive.	
6.4	**Resilience**	
Description	*Resilience refers to the capability of a FinTech organisation to tolerate and recover from cybersecurity incidents or disruptions effectively.*	
	Guidelines	
6.4.1	Implement measures that prevent, detect, respond to, and restore from security breaches. This includes incident response planning, business continuity management, data backup and recovery procedures, and periodic testing and evaluation of these processes.	
6.4.2	Ensure that FinTech organisations can quickly mitigate the impact of cybersecurity incidents and restore routine activities.	

Figure 6.2 depicts the final version of the proposed cybersecurity framework for FinTech in Bahrain (CFFB).

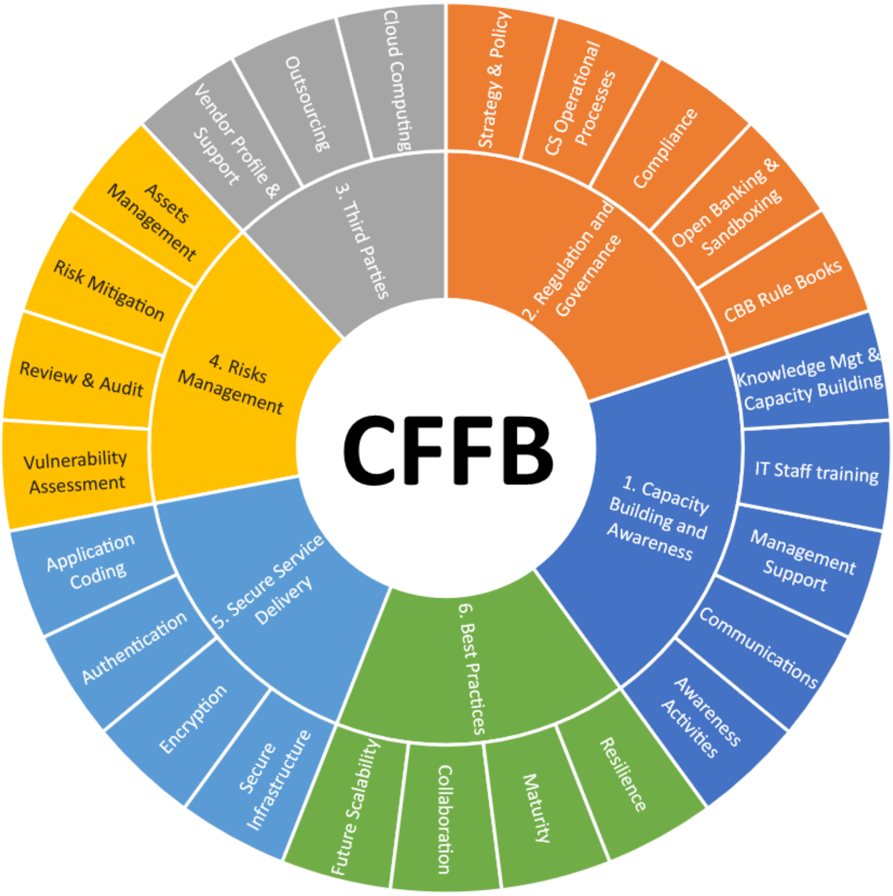


Figure 6.2 Final Version of the CFFB Framework.

6.3. CFFB's Controls Mapping to the International Cybersecurity Standards

The proposed framework shares a common goal of enhancing data security of FinTech systems. This section maps the framework’s controls to cybersecurity international standards, namely NIST, ISO 27001, COBIT, and PCI-DSS. It provides a resource for stakeholders to use in understanding how to align these controls to meet their objectives.

FinTech may use the mapping in Table 6.8 to discover opportunities for enhancing control efficiency and achieving more alignment across international cybersecurity standards. For instance, mapping may assist in determining the areas where the use of a certain control can contribute to achieving the desired result of the standard. Moreover, FinTech may use its own evaluations to check the efficacy of enforced controls, so enabling them to be better prepared for any standards assessment. By using this approach, the mapping facilitates a uniform and synchronised strategy for cybersecurity throughout the FinTech entities.

Table 6.8 Mapping Framework's Controls to the International Cybersecurity Standards

Principle	Controls	NIST	ISO 17799	COBIT	PCI-DSS
Capacity Building and Awareness	Awareness Activities	PR.AT-1/2/3/4	A.7.2.2, A.12.2.1	APO07.03, BAI05.07	6.7, 7.3, 8.4, 9.9.3, 12.4, 12.6
	Communications	ID.AM-3 RC.CO-1/2/3	A.13.2.1 A.6.1.1, A.7.2.2, A.16.1.1	DSS05.02 DSS03.04 EDM03.02 EDM03.02, APO01.02, APO12.03	1.1.2, 1.1.3 12.10.6 12.10
	Management Support	PR.AT-4	A.6.1.1, A.7.2.2,	APO07.03	12.5
	IT Staff training	AT-3, PR.AT-1	A.7.2.2	APO07.03, BAI05.07	6.5, 9.9.3, 12.4, 12.6
	Knowledge Mgt & Capacity Building	RS.IM-1/2 RC.IM-1	A.16.1.6	BAI01.13 BAI05.07	12.10.6
Regulation and Governance	CBB Rule Books	PR.IP-5	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3	DSS01.04, DSS05.05	9 (all)
	Open Banking and Sandboxing	-	-	-	-
	Compliance	-	-	-	-
	Operational Processes	PR.IP RC.RP RS.MI RS.AN-5 DE.DP -2/3	A.18.1.4, A.18.2.2, A-18.2.3 A.7.2.2	APO12.06, DSS03.02, DSS05.07 EDM03.02 DSS06.01, MEA03.03, MEA03.04 APO13.02, DSS05.02	11.5.1, 12.5.2 6.1, 6.2 10.9, 11.2, 11.3, 11.4, 12.10.1 10.6.1

Principle	Controls	NIST	ISO 17799	COBIT	PCI-DSS
	Strategy & Policy	ID.GV-1	A.5.1.1	APO01.03, EDM01.01, EDM01.02	1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6, 12.1
Third Parties	Cloud Computing	-	-	-	Appendix A1
	Outsourcing	-	-	-	-
	Vendor Profile & Support	PR.AT-3	A.6.1.1, A.7.2.1, A.7.2.2	APO07.03, APO07.06, APO10.04, APO10.05	2.6, 12.8, 12.9
Risks Management	Assets Management	ID.AM-1/2	A.8.1.1, A.8.1.2	BAI09.01, BAI09.02, BAI09.05	2.4, 9.9, 11.1.1 12.3.3
	Risk Mitigation	ID.RM-1/2 RS.MI-2	Clause 6.1.3, Clause 8.3, Clause 9.3 A.12.2.1, A.16.1.5	APO12.06	12.2 11.5.1, 12.5.2
	Review & Audit	PR.PT-1	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	APO11.04	10.1, 10.2, 10.3, 10.6.1, 10.6.2
	Vulnerability Assessment	ID.RA-1	A.12.6.1, A.18.2.3	APO12.01, APO12.02, APO12.03, APO12.04	6.1, 11.2, 11.3 12.2
Secure Service Delivery	Application Coding	PR.IP-2	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5	APO13.01, BAI03.01, BAI03.02, BAI03.03	6.3, 6.4, 6.5, 6.6, 6.7
	Authentication	PR.AC-1	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4,	DSS05.04, DSS06.03	2.1, 8.1, 8.2, 8.5, 8.6, 12.3

Principle	Controls	NIST	ISO 17799	COBIT	PCI-DSS
			A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3		
	Encryption	PR.DS-1/2/5	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	APO01.06, DSS06.06	4.1, 4.2, 4.3
	Secure Infrastructure	PR.PT-4	A.13.1.1, A.13.2.1	DSS05.02, APO13.01	1 (all), 2 (all), 4.1
Best Practices	Future Scalability				
	Collaboration	RS.CO-4/5	Clause 7.4 A.6.1.4	BAI08.04	12.10.1
	Maturity				
	Resilience	PR.IP-9	A.16.1.1, A.17.1.1, A.17.1.2	DSS04.03	11.1.2, 12.5.3, 12.10

Counting the number of intersecting controls between CFFB and NIST, ISO 17799, COBIT, and PCI-DSS standards leads to the visual illustration as in Figure 6.3.

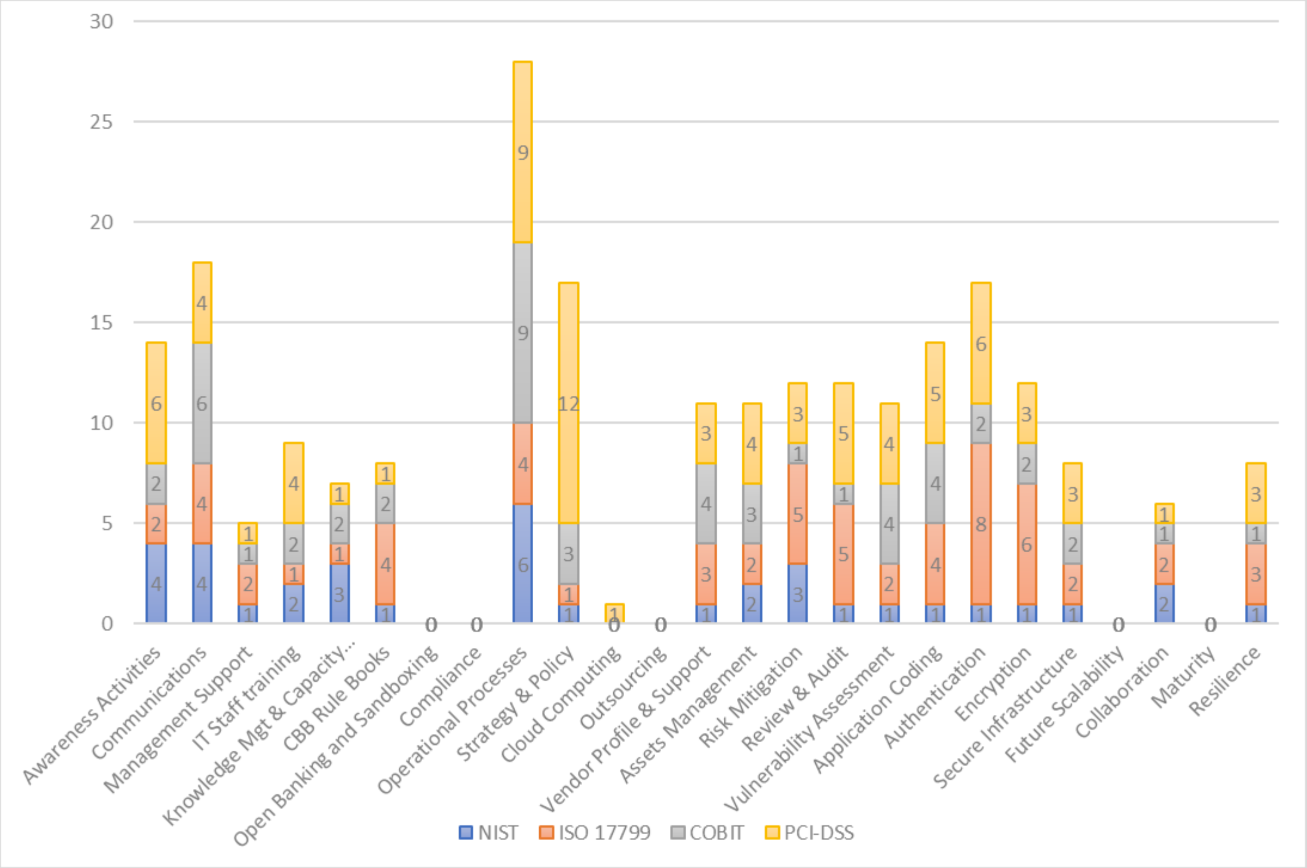


Figure 6.3 Number of intersecting controls with CFFB

Open Banking and Sandboxing, Compliance, Outsourcing, Future Scalability, and Maturity have scores of 0 across all standards, indicating that these control categories are not addressed well or considered in the given standards. CFFB provides clear guidance and control in these areas as these are specific to Bahrain's FinTech needs. Management Support has only one control in NIST, COBIT, and PCI-DSS, indicating that the level of emphasis on management support is relatively low in these standards. CBB Rule Books, which incorporate other national regulations and laws, have a score of 1 in NIST and PCI-DSS, indicating a relatively lower emphasis on this control category in these standards. Cloud Computing has only 1 control in PCI-DSS and 0 in other standards, indicating a lower emphasis on addressing security control on cloud computing for FinTech. Outsourcing has scores of 0 across all standards, indicating that the standards may not provide specific guidance for managing outsourcing risks. ISO 17799 is highly concerned about the Authentication and secure access controls to the FinTech systems. All standards and CFFB is concentrating on Operational Processes since they encompass the day-to-day activities and procedures involved in managing and protecting FinTech's information systems and data. Since PCI-DSS focuses on payment processes, it is clear the higher number of controls are intersecting with CEEB's controls. Avoiding the complexity and lengthy controls, CFFB focuses in highlighting comprehensive easy to implement controls across its 6 principles. It contributes extra features to the implementation of any international standards if FinTech firm is mandated to comply with. When implemented correctly, this will facilitate compliance and resilience with ongoing regulatory requirements.

6.4. Evaluation of Research Question

The study's research question is stated clearly in the first chapter, which was "**What are the crucial elements in developing a Cybersecurity Framework designed for FinTech entities in Bahrain?**". The research question focuses on the cybersecurity challenges faced by the FinTech industry in Bahrain and the development of appropriate measures to manage FinTech cyber risks. The research also aims to propose a cybersecurity framework specific to the FinTech ecosystem in Bahrain. By focusing on the crucial elements of a cybersecurity framework, the research question highlights the need to identify and address the specific requirements and challenges faced by FinTech entities in Bahrain.

The increasing reliance on digital platforms and the growing sophistication of cyber threats pose significant risks to the integrity, privacy, and trustworthiness of FinTech services (AlBenJasim et al., 2023). By focusing on the intersection of FinTech and cybersecurity, the research question acknowledges the need for robust cybersecurity measures to mitigate these risks and ensure the sustainable growth of the FinTech sector in Bahrain.

The research question is specific to the context of Bahrain's FinTech ecosystem, which is appropriate given the goal of developing a cybersecurity framework tailored to the unique characteristics and challenges of Bahrain's FinTech industry. This specificity enhances the practical relevance and applicability of the research findings to the local FinTech stakeholders. Furthermore, the research question aligns with the stated core contribution of the research, and it guides the research process and ensures that the research outcomes directly address the identified gap in knowledge. It addresses a significant gap in the field of FinTech cybersecurity and sets the foundation for the subsequent research activities, including the literature review, methodology, data analysis, and validation of the proposed framework.

6.5. Fulfilment of Research Objectives

The purpose of this research is to investigate the challenges faced by the financial technology (FinTech) industry in the context of cybersecurity, and to develop a cybersecurity framework that addresses the unique characteristics and challenges of the FinTech ecosystem in Bahrain, with the goal of ensuring the sustainable growth of the sector while fostering trust and confidence in the use of FinTech innovations.

To fulfil this research purpose, the following key objectives were pursued:

No	**Research Objectives**	Fulfilment
1	**Identify the cybersecurity challenges encountered by the FinTech industry worldwide and specifically in Bahrain.**	The research carried out an SLR to investigate the current state of FinTech and its associated cybersecurity challenges. This included an analysis of risks, countermeasures, and different types of cyber threats in the FinTech ecosystem. The objective was to gain a comprehensive understanding of the existing challenges. A research SLR paper was published.
2	**Investigate commonly adopted cybersecurity standards in the financial sector worldwide.**	The research examined the cybersecurity standards and frameworks commonly utilised in the financial industry globally. This analysis aimed to identify best practices and establish a foundation for developing a cybersecurity framework tailored explicitly to the FinTech sector in Bahrain.
3	**Data collection by interviewing experts.**	Primary data collection was done through expert interviews. The interviews designed to gather information about challenges facing FinTech businesses and investigating the common cybersecurity practices for incident response plans, vulnerability management practices, prevention actions, and the assessment of end users' behaviors and skills related to cybersecurity in the FinTech sector in Bahrain.
4	**Analyse and develop a cybersecurity framework for FinTech stakeholders in Bahrain.**	Based on the identified challenges and the analysis of existing standards, the research proposed a cybersecurity framework designed explicitly for the FinTech ecosystem in Bahrain. The framework encompassed key principles such as Regulation and Governance, Capacity Building and Awareness, risk management, Secure Service Delivery, Best Practices, and Third Parties. The

		objective was to provide a comprehensive and practical framework to manage cybersecurity risks in FinTech.
5	**Validate the proposed framework and its applicability through expert consultation.**	The research employed the focus group review and Delphi rounds techniques to validate the proposed cybersecurity framework. Key stakeholders in the FinTech industry in Bahrain were consulted to review and assess the applicability of the framework. This validation process aimed to ensure that the framework adequately addressed the unique challenges and requirements of the FinTech industry in Bahrain.

The fulfilment of the research purpose involved conducting a comprehensive literature review, developing a tailored cybersecurity framework, validating the framework through expert consultation, analysing the research outcomes, and providing recommendations for further study. The research aimed to contribute to the sustainable growth of the FinTech sector in Bahrain by addressing cybersecurity risks and fostering trust in FinTech innovations.

In the next sections, some suggestions for further study based on the research findings are presented. These recommendations aimed to guide future research efforts in the field of FinTech cybersecurity and its intersection with the regulatory and governance landscape. Additionally, the implications of the research findings for other jurisdictions facing similar challenges are discussed, emphasising the potential value of the developed framework as a reference for future endeavours.

6.6. Research Contributions

Financial regulators are being forced to introduce new guidelines in order to protect against cyberattacks occurring in the financial industry as a consequence of cybercrime threats. The CFFB presented in this research includes controls that will benefit FinTech stakeholders. The results of this research may be used by the CBB to enhance cybersecurity regulations for FinTech in Bahrain.

FinTech corporate executives, leaders, and managers will benefit from the framework proposed in this research. These professional experts are in charge of putting cybersecurity policies in place at their FinTech must understand that in order to properly execute cybersecurity plans, its workers must be competent, have enough training, and be well aware of cybersecurity concerns. Furthermore, the outcomes of the research enable leaders to assist their workforce while adhering to cybersecurity standards. IT professionals with cybersecurity knowledge, awareness, and training are better suited to deal with cybersecurity threats.

During interviews and discussions with experts, it was determined that this insufficiency of preventive cybersecurity measures in Bahrain's FinTech institutes was partially due to the absence of a meaningful framework as well as a checklist to evaluate the efficacy of the cybersecurity controls within these entities. FinTech must address this shortcoming with appropriate actions in order to achieve a robust security stance. This work adds to the body of knowledge by establishing a helpful cybersecurity framework in Bahrain's FinTech institutions.

Existing cybersecurity standards, which primarily concentrate on technology processes for risk identification, detection, prevention, and analysis, have a gap in addressing other factors related to Bahrain's FinTech institutes. Others were judged to be insufficient due to a concentration on European or American norms, which may not completely address cybersecurity challenges in Bahrain's regulation setting. Furthermore, these frameworks were found to be complicated, mainly in terms of interpretation and execution. As a result, the researcher proposed the latest innovative techniques to supplement the current ones. This includes implementing culturally relevant cybersecurity training and awareness programs. These programs should suit the local culture of people in Bahrain when it comes to social engineering tricks and the treatment of personal data. All of these innovative techniques and recommendations will ensure a solid legislative structure, effective governance support, and the recruitment and retention of skilled information technology experts in FinTech entities, as well as the integration of cybersecurity strategies into the overall FinTech ecosystem.

Therefore, a robust cybersecurity framework for the FinTech sector in Bahrain will contribute to the overall economic development and investor confidence in the country. By demonstrating a commitment to cybersecurity and providing a secure environment for FinTech operations, Bahrain can attract more international investments, foster innovation, and position itself as a trusted FinTech hub in the region. The research will contribute to the long-term sustainability and competitiveness of Bahrain's FinTech industry.

6.7. Novelty of the Research Work

What sets this framework apart is its adaptability and flexibility. It considers the rapidly evolving nature of the FinTech industry and the ever-changing cyber threat landscape. The framework is designed to be dynamic, allowing continuous updates and adjustments to address emerging risks and vulnerabilities effectively. This adaptability ensures that it remains relevant and effective over time, providing a sustainable and robust cybersecurity solution for the FinTech ecosystem in Bahrain.

The evaluation of the framework's practical feasibility, risk mitigation capabilities, and compatibility with existing regulatory frameworks through panel discussions and Delphi sessions further highlights its potential. Industry experts with extensive knowledge and experience in the FinTech sector have recognised the significance of the CFFB framework. Their high acceptance and endorsement indicate that the framework has the potential to make a substantial impact in enhancing cybersecurity resilience within the FinTech industry in Bahrain.

In section 6.3, Open Banking and Sandboxing, Compliance, Future Scalability, and Maturity have scores of 0 across all standards, indicating that these control categories are not addressed well or considered in the given standards. CFFB provides clear guidance and control in these areas, which are specific to Bahrain’s FinTech needs. Moreover, Outsourcing has scores of 0 across all standards, indicating that the standards may not provide specific guidance for managing outsourcing risks. Avoiding the complexity and lengthy controls, CFFB focuses in highlighting comprehensive easy to implement controls across its 6 principles. It contributes extra features to implementing any international standards that a FinTech firm is mandated to comply with. When implemented correctly, this will facilitate compliance and resilience with ongoing regulatory requirements.

While the proposed CFFB was presented in July 2022 during the Internal Evaluation IE assessment, in August 2023, the NIST published a preliminary version of its Cybersecurity Framework (CSF) 2.0, marking the first major update since its 2014 release (Boutin, 2023). The update aims to make the framework more accessible and practical for all organisations, not just critical infrastructure sectors. The scope has expanded to include organisations of all sizes and sectors rather than focusing solely on critical infrastructure. Additionally, a new "**govern**" function has been added as the sixth pillar of a successful cybersecurity program, emphasising cybersecurity as a significant enterprise risk. Therefore, this research aligns with the changes proposed by NIST in its CSF 2.0 draft. The addition of the **governance** element as a sixth pillar recognises the importance of cybersecurity as a major enterprise risk and emphasises the involvement of senior leadership. This aligns with our findings, which indicate that strong governance and executive support are crucial for effective cybersecurity practices. Furthermore, the expanded scope of the framework to include organisations of all sizes aligns with our research on the suitability of CFFB for different FinTech business sizes. This recognition of the diverse needs and capabilities of FinTech organisations will allow for greater flexibility and applicability of the CFFB in the FinTech sector.

6.8. Future Research and Recommendations

The study utilises a qualitative methodology to get insights into the significant aspects that impact the development of the CFFB. The FinTech sector in Bahrain has a proactive approach towards the adoption of cutting-edge technology. However, it is crucial to do additional research on this dynamic and innovative field due to the industry's heavy dependence on technology solutions.

The suggestions for future research include both those that have been directly drawn from the information gathered during this research, along with those that have been formulated via careful analysis of the research findings, research focus group discussions, and the Delphi workshop. During the interview sessions, the participants in certain cases also offered suggestions for ideas for further studies. Four key recommendations were generated from all these sources.

Firstly, the perceived effectiveness when implementing the framework at FinTech firms. Secondly, to incorporate Artificial Intelligence (AI) technologies into the CFFB’s controls and processes and measure the impact. Thirdly, to replicate the study in a different demographic to further explore extended findings. Lastly, extending the scope of the research topic.

6.8.1. Effectiveness of Implementing the Framework

As the field of cybersecurity in the FinTech sector continues to evolve, it becomes crucial to evaluate the effectiveness of implementing the proposed CFFB specific to the context of Bahrain. Future research can investigate the extent to which the framework incorporates mechanisms for continuous monitoring, assessment, and improvement. This can involve examining the agility of the framework in responding to emerging threats, the effectiveness of incident response and recovery mechanisms, and the ability to integrate new technologies and best practices.

To assess the effectiveness of the CFFB in Bahrain, it may be valuable to conduct a comparative analysis with frameworks implemented in some FinTech entities. Such a comparative analysis can identify strengths, weaknesses, and potential areas for improvement specific to the Bahraini FinTech. Evaluating the effectiveness of the framework may require a combination of quantitative and qualitative analysis. Quantitative analysis can involve statistical techniques to measure the impact of the framework on reducing vulnerabilities and mitigating cyber risks. Qualitative analysis can include interviews, surveys, and case studies to gather insights from industry stakeholders, regulators, and FinTech organisations regarding their experiences and perceptions of the CFFB's effectiveness.

6.8.2. Integrating Artificial Intelligence (AI) into CFFB's Controls and Processes

Artificial Intelligence (AI) technology, possess the power to greatly enhance the detection and response capabilities of cybersecurity systems (Ali et al., 2020). The integration of AI technologies into cybersecurity controls and processes holds great potential for enhancing the effectiveness and efficiency of the CFFB. By exploring areas such as threat detection and response, behavioural analysis, automated security operations, adaptive systems, ethical considerations, and evaluation metrics, future research can contribute to harnessing the power of AI to strengthen the cybersecurity defences of the FinTech ecosystem in Bahrain while addressing associated challenges and ensuring responsible and trustworthy AI implementation.

6.8.3. Replicating the Study in Different Characteristics

Conducting the research study in different demographics, such as another country or region, allows for a broader understanding of how cybersecurity frameworks operate in diverse contexts. Different characteristics may have distinct regulatory frameworks, cultural factors, and technological landscapes that can impact the implementation and effectiveness of cybersecurity controls in the FinTech sector. Future studies in replicating this research in different characteristics offer valuable insights into the generalizability and contextual applicability of the findings. By considering the diversity of characteristics, cross-cultural perspectives, regulatory variations, and technological infrastructure and conducting comparative analysis, future research can advance our understanding of cybersecurity practices in the FinTech industry across different regions. The insights gained from such replication studies can aid in generating tailored and efficient (International) cybersecurity frameworks that address the specific needs and challenges of FinTech in various demographics.

6.8.4. Extending the Scope of the Research Topic

The dynamic nature of the cybersecurity landscape necessitates continuous research to address emerging technologies and threats, where extending the scope of the research topic opens new avenues for exploration and addresses emerging challenges. Future studies can focus on investigating the implications of emerging technologies. By exploring the unique security challenges and vulnerabilities associated with these technologies, researchers can propose innovative approaches and countermeasures to enhance the resilience of the FinTech ecosystem.

Moreover, incorporating a user-centric perspective into the CFFB can be a valuable direction for future research. This involves examining the usability of security measures, user awareness, and user behaviour within the FinTech sector in Bahrain. Understanding the human factors and user experiences associated with cybersecurity can help identify potential weaknesses and design interventions to promote secure practices among users.

Such future research can contribute to the ongoing development and enhancement of the CFFB. The insights gained from extending the research scope can guide policymakers, industry practitioners, and regulators in effectively addressing the evolving cybersecurity landscape within the FinTech sector in Bahrain.

6.9. Conclusion

In conclusion, the proposed cybersecurity framework in this thesis represents a significant novelty in addressing the unique requirements of the FinTech industry in Bahrain. While existing literature primarily focuses on general cybersecurity practices and frameworks, this research explicitly targets the FinTech sector, recognising its distinct characteristics and vulnerabilities.

The FinTech industry operates in a complex landscape involving collecting and sharing sensitive financial data. This data includes personal and financial information of individuals and organisations, making it a prime target for cybercriminals. Additionally, the involvement of multiple users in FinTech platforms introduces additional complexities regarding access control and user authentication. Time-sensitive transactions are another critical aspect of the industry, where delays or disruptions can have severe financial consequences for both businesses and customers. One of the challenges encountered by FinTech businesses is the relatively low investment in Information Technology (IT) and cybersecurity compared to traditional financial institutions. This can lead to vulnerabilities in systems and processes, making them attractive targets for cyberattacks. Furthermore, the potential for significant financial harm in the event of a successful cyberattack adds urgency to the need for robust cybersecurity measures. Information imbalances between customers and providers also present challenges in the FinTech industry. Customers may not possess equivalent levels of awareness of cybersecurity threats compared to the service providers. Malicious actors can exploit this imbalance, leading to unauthorised access, data breaches, or fraudulent activities. Another crucial consideration is the broader financial and regulatory context within which each FinTech operates. National legislation, financial industry governance, and regulatory guidelines play a significant role in shaping the cybersecurity readiness of FinTech firms. Adapting to these regulatory requirements while maintaining security can be a complex task that requires a dedicated and tailored approach.

Developing a FinTech sector-specific cybersecurity framework that is simple, flexible, and adaptable becomes crucial in addressing these unique characteristics and challenges. By identifying and integrating components, processes, and activities that were previously overlooked or missed in existing international standards, this research contributes to filling these gaps.

To bridge these gaps, this study undertakes a qualitative research approach to address the problem. It begins by conducting an extensive review that delves into the realm of cybersecurity, encompassing an examination of the current challenges, common practices, and established cybersecurity standards. By thoroughly analysing these aspects, the research gains a comprehensive understanding of the cybersecurity landscape and identifies the key areas that require attention within the FinTech industry in Bahrain.

To further enhance the research's depth and insight, in-depth research interviews are conducted with professionals who possess valuable expertise and insights in the FinTech domain. This includes executives, experts, and other stakeholders intimately involved in the FinTech business ecosystem. Engaging with these knowledgeable experts gives the researcher access to firsthand experiences, industry perspectives, and practical insights that enrich the research findings and recommendations.

Leveraging the knowledge gathered, this research employs a qualitative analysis approach, utilising insights from extensive research interviews. It incorporates contextual understanding, real-world challenges, and industry expertise, ensuring a holistic view of the cybersecurity landscape within the FinTech ecosystem in Bahrain. The research identifies patterns, themes, and trends by synthesising the qualitative data, providing valuable insights for the proposed framework.

Incorporating these qualitative findings and analysing data through an STS lens revealed patterns, relationships, and themes that contribute to cybersecurity controls within the industry. Building on the research findings, the STS theoretical model facilitated the synthesis of the knowledge gained to develop a comprehensive cybersecurity framework for the FinTech industry. The framework emphasised the importance of considering technology, people, and operational factors in an integrated manner. The research proceeded to propose a novel and adaptable framework that aligned with industry experiences, increasing its potential effectiveness in mitigating identified risks and vulnerabilities. It considered the specific context, challenges, and dynamics of the FinTech industry in Bahrain, ensuring that the framework is tailored to meet the precise needs of this particular ecosystem.

Therefore, the proposed Cybersecurity Framework for FinTech in Bahrain (CFFB) aimed to provide comprehensive guidance to ensure effective control of cyber risks and optimise the use of FinTech assets.

The (CFFB) encompassed various elements to address the sector's specific needs. It covered areas such as awareness activities, IT staff training, knowledge management, capacity building, regulation and governance, secure service delivery, secure application coding, authentication, encryption, secure infrastructure, risk management, assets management, risk mitigation, review and audit, vulnerability assessment, third parties, cloud computing, outsourcing, vendor profile and support, future scalability, collaboration, maturity, and resilience. The CFFB comprised six principles and involved twenty-five control activities detailed in fifty guidelines, adopting a risk-based methodology to address current and future technological advancements and potential threats.

To ensure the effectiveness and applicability of the framework, it underwent a rigorous review process involving cybersecurity experts from banking and FinTech businesses. The framework's components were reviewed, validated, refined, and ranked through group reviews and Delphi techniques. This iterative process not only enhanced the framework but also made the controls more straightforward for implementation and more usable for different sizes of FinTech innovations.

The adoption of the CFFB framework is anticipated to have a profound impact on various stakeholders. FinTech businesses will benefit from increased cybersecurity resilience, protecting their systems, customer data, and reputation. Policymakers and regulators will have a comprehensive framework to guide their decision-making and ensure the security and stability of the FinTech industry. National security will be strengthened as the framework mitigates the risk of cyberattacks that can have broader implications for the economy and society. International collaboration can be fostered by aligning Bahrain's cybersecurity standards with global best practices, promoting cross-border trust and cooperation. Overall, the framework contributed to the sustainable growth of the FinTech sector, boosting investor confidence and economic development in Bahrain.

What sets this framework apart is its adaptability and flexibility. It considered the rapidly evolving nature of the FinTech industry and the ever-changing cyber threat landscape. The framework was designed to be dynamic, allowing continuous updates and adjustments to address emerging risks and vulnerabilities effectively. This adaptability ensures that it remains relevant and effective over time, providing a sustainable and robust cybersecurity solution for the FinTech ecosystem in Bahrain.

The evaluation of the framework's practical feasibility, risk mitigation capabilities, and compatibility with existing regulatory frameworks through panel discussions and Delphi sessions further highlighted its potential. Industry experts with extensive knowledge and experience in the FinTech sector have recognised the significance of the CFFB framework. Their high acceptance and endorsement indicate that the framework has the potential to create a significant influence in enhancing cybersecurity resilience within the FinTech industry in Bahrain.

The potential of this research goes beyond addressing immediate FinTech cybersecurity challenges. By filling the gap in the literature and providing a tailored framework, it contributed to the establishment of an ideal, secure, and streamlined environment for FinTech innovations in Bahrain. This, in turn, fosters a conducive ecosystem that encourages further growth and development of the FinTech industry. With a robust cybersecurity framework, FinTech companies in Bahrain could operate with increased confidence, knowing that their systems and data are protected.

Furthermore, adopting CFFB facilitated Bahrain's commitment to embracing technology-driven changes while prioritising security. This commitment strengthened Bahrain's reputation as a secure destination for FinTech, which can positively affect the overall economy. The presence of a robust cybersecurity framework not only protects the FinTech industry but also promotes trust and confidence among customers, investors, and other stakeholders. This can attract both local and international businesses to establish their operations in Bahrain, positioning the country as a regional FinTech hub.

6.10. Study Limitations

A significant constraint of qualitative research is the context-specific nature of its results, which hinders their generalizability to broader populations. Qualitative research often uses a limited sample size, sometimes lacking in the ability to adequately capture the range of viewpoints found among a larger community. Hence, it is essential to use caution when endeavouring to extrapolate qualitative results to a broader population or form broad generalisations (Harper, 2013).

A cybersecurity framework for FinTech entities in Bahrain has been proposed in this study. The study utilised a qualitative methodology to get insights into the significant aspects that impact the development of a cybersecurity framework for FinTech businesses in Bahrain. However, it was vital to note that the findings may not be generalisable in a statistical context. In order to effectively address this issue, it was highly suggested that future research endeavours include a variety of methodologies and encompass a wide range of quantitative perspectives.

Another limitation of this research was the restricted accessibility and unavailability of data concerning FinTech cybersecurity incidents since these occurrences are handled with utmost confidentiality by most FinTech companies.

In addition, this study acknowledged limitations in its generalisability by specifying its focus on FinTech entities in Bahrain. Cybersecurity concerns could differ depending on factors like industry, culture, local regulations, and the threat landscape of a particular country.

The research could be strengthened by comparing cybersecurity risks, policies, attack patterns, level of awareness, and responses to similar threats faced by FinTech businesses in other countries. This comparative review would help clarify whether the findings specific to Bahrain hold true for a broader range of FinTech firms globally or require contextualisation for Bahrain's unique case.

In essence, the research established the baseline for a more comprehensive understanding of cybersecurity in the FinTech industry. By including factors from other nations, researchers can determine whether the challenges faced by Bahrain's FinTech industry are universal or require a Bahrain-specific approach.

6.11. Reflection on the Research Work

Completing a PhD means spending ample hours researching, thinking, and writing. Here, I am reflecting briefly on the research journey, highlighting some of the key challenges and lessons that emerged, and the personal skills I developed through this work.

6.11.1. Great Supervision

I am so grateful for the support and direction received from my supervisors during my PGR journey. Their devotion to my research development has created an atmosphere for my research growth and success.

They thoroughly comprehended my research topic and supplied vital guidance and instructions at the early stages. Their extensive experience in supervision and knowledge has enhanced my research and challenged me to try new things. They promoted independent thinking and inventiveness, helping me establish my research voice and significantly contributing to my research work.

6.11.2. Challenges

The research clearly highlights a significant need in the current body of knowledge about a cybersecurity framework for the FinTech sector, notably in relation to Bahrain. To fill this gap, an extensive review of current cybersecurity standards was necessary to collect specific knowledge relevant to the business. The research highlights the significance of ensuring that the proposed framework aligns with the current regulatory environment for FinTech in Bahrain. Ensuring the framework's practical application and broader acceptance throughout the sector was a significant issue, requiring careful navigation and alignment with regulatory constraints.

In addition, the FinTech industry must always be vigilant and flexible to handle the constantly evolving realm of cybersecurity risks successfully. In order to maintain the relevance and effectiveness of the proposed framework, it is essential to continually monitor, analyse, and periodically alter it to address emerging threats and advancements in technology.

6.11.3. Lessons Learned

The FinTech sector is characterised by its own specific features, which need the adoption of a focused strategy in order to effectively address rising cyber threats. In the course of my research, I discovered that general cybersecurity standards have some limitations and that there is a need for a framework that is focused on FinTech.

The research approach demonstrates the value of industry collaboration and the incorporation of diverse perspectives. This collaborative approach ensures that the proposed framework is practically feasible and acceptable, addresses specific risks, and aligns with the existing FinTech ecosystem in Bahrain.

6.11.4. Personal Skills

Several of my personal skills were developed and refined over the course of this research journey. First, addressing the evolving technologies both for the FinTech landscape and emerging cybersecurity threats required me to be adaptable and flexible in my research approach. Adjusting the research methodology and framework to accommodate industry feedback and aligning with the changing regulatory environment resulted in the ability to adapt to new circumstances. Second, interacting with different stakeholders to collect various perspectives and incorporate their feedback into the research enhanced my ability to work effectively in a collaborative environment. Moreover, my communication skills developed while conducting interviews and leading panel discussions. Furthermore, to clearly present and explain the proposed framework and its practical feasibility to different stakeholders enhanced my interpersonal capabilities. Third, the research depended on an extensive review of existing cybersecurity standards, which led me to pay attention to detail and commit to a rigorous research outcome. In addition, ensuring the proposed framework's practical feasibility and ability to address cyber risks forced me to pay full attention to the details. Finally, one important skill that I acquired is resilience and persistence in various research challenges. Overcoming these difficulties produced a well-received, adaptable framework and highlighted my determination and ability to persevere through complex research issues.

References

7. References

(ECB), E. C. B. (2017). Guide to assessments of fintech credit institution licence applications. *European Central Bank*, *Banking Supervision*.

Abdelghani, E., Mohammed Mispah Said, O., Abdullah Mohammed, A., & Welcome, S. (2021). Islamic Banks Financing of FinTech Start-Ups in Oman: An Exploratory Study. *The Journal of Muamalat and Islamic Finance Research*, *18*(1), 55-65. https://doi.org/10.33102/jmifr.v18i1.329

Abdulkarim, A. M. (2021). Bank Users Motivation for Adoption of Fintech Services: Empirical Evidence with TAM in Kingdom of Bahrain. *iKSP Journal of Innovative Writings*, *1*(2).

Abdullah, E. M. E., Rahman, A. A., & Rahim, R. A. (2018). Adoption of financial technology (Fintech) in mutual fund/unit trust investment among Malaysians: Unified Theory of Acceptance and Use of Technology (UTAUT). *International Journal of Engineering and Technology (UAE)*, *7*(2), 110-118.

Ahmed, A. S., Kumar, M., & Moh'd Ali, M. A. (2020). Adoption of FinTech and Future Perspective: An Empirical Evidence from Bahrain on Digital Wallets. 2020 International Conference on Decision Aid Sciences and Application (DASA),

Al-Ahmad, W., & Mohammad, B. (2012). Can a single security framework address information security risks adequately. *International Journal of Digital Information and Wireless Communications*, *2*(3), 222-230.

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. *Journal of Xidian University*, *14*(7), 1523-1536.

Al-Alawi, A. I., & Al-Bassam, S. A. (2021). Assessing The Factors of Cybersecurity Awareness in the Banking Sector. *Arab Gulf Journal of Scientific Research*.

Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020). Critical Cybersecurity Threats: Frontline Issues Faced by Bahraini Organizations. In *Implementing Computational Intelligence Techniques for Security Systems Design* (pp. 210-229). IGI Global.

Al-Alawi, A. I., Al-Hammam, A. H., Al-Alawi, S. S., & AlAlawi, E. I. (2021). The Adoption of E-Wallets: Current Trends and Future Outlook. In *Innovative Strategies for Implementing FinTech in Banking* (pp. 242-262). IGI Global.

Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: a review cases in cyber-physical systems. *Int. J. Adv. Comput. Sci. Appl*(1), 499-508.

Al-Shakar, A. (2017). Entrepreneurship: A New Era for Bahrain's Economy? *Global Policy*, *8*(3), 413-416. https://doi.org/10.1111/1758-5899.12483

Al Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science*, *9*(6), 123-133.

Al Sabbagh, B. (2019). *Cybersecurity incident response: a socio-technical approach* Department of Computer and Systems Sciences, Stockholm University].

Al Sabbagh, B., & Kowalski, S. (2015). A socio-technical framework for threat modeling a software supply chain. *IEEE Security & Privacy*, *13*(4), 30-39.

Albastaki, Y., & Manta, O. (2020). *Innovative Strategies for Implementing FinTech in Banking Book*.

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. *Journal of Computer Information Systems*, 1-17.

Ali, H., Al Kaabi, R., Ali, H. M., Ahmed, H. S., & Naser, M. (2021). FinTech in the Kingdom of Bahrain: An Investigation of Users' Adoption and Satisfaction. In *Innovative Strategies for Implementing FinTech in Banking* (pp. 174-190). IGI Global.

Ali, R., Ali, A., Iqbal, F., Khattak, A. M., & Aleem, S. (2020). A Systematic Review of Artificial Intelligence and Machine Learning Techniques for Cyber Security. In Y. Tian, T. Ma, & M. K. Khan (Eds.), *1st International Conference on Big Data and Security, ICBDS 2019* (Vol. 1210 CCIS, pp. 584-593): Springer.

America, B. o. (2019). Risk management and cyber security framework. *global institutional consulting*. https://mediahandler.broadridgeadvisor.com/media/267992/RiskManagement.pdf

Ancri, C. (2016). Fintech innovation: An overview. *Presentation, Board of Governors of the Federal Reserve System, Washington, DC (October 19)*.

Ani, U. D., Watson, J. M., Tuptuk, N., Hailes, S., & Jawar, A. (2023). Socio-technical security modelling: analysis of state-of-the-art, application, and maturity in critical industrial infrastructure environments/domains. *arXiv preprint arXiv:2305.05108*.

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management decision*, *35*(6), 452-463.

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, *11*, 305.

Babazadeh, Y., Frahamand, F.-h., Pasebani, M., & Alavi Matın, Y. (2022). Identifying key indicators for developing the use of blockchain technology in financial systems. *International journal of research in industrial engineering*, *11*(3), 246-257.

Barahona, D. (2022). Cybersecurity in Fintech: Top 8 FinTech Cybersecurity Risks and Challenges. https://www.apisec.ai/blog/fintech-cybersecurity-risks-and-challenges

Barbu, C. M., Florea, D. L., Dabija, D.-C., & Barbu, M. C. R. (2021). Customer experience in fintech. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1415-1433.

Barlette, Y., & Fomin, V. V. (2010). The adoption of information security management standards: A literature review. *Information Resources Management: Concepts, Methodologies, Tools and Applications*, 69-90.

Basole, R. C., & Patel, S. S. (2018). Transformation through unbundling: Visualizing the global FinTech ecosystem. *Service Science*, *10*(4), 379-396.

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2021). Data breach investigations report. *Verizon DBIR Team, Tech. Rep*.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with computers*, *23*(1), 4-17.

Bazen, A., Barg, F. K., & Takeshita, J. (2021). Research techniques made simple: an introduction to qualitative research. *Journal of Investigative Dermatology*, *141*(2), 241-247. e241.

Beiderbeck, D., Frevel, N., von der Gracht, H. A., Schmidt, S. L., & Schweitzer, V. M. (2021). Preparing, conducting, and analyzing Delphi surveys: Cross-disciplinary practices, new directions, and advancements. *MethodsX*, *8*, 101401.

BFB. (2018). Bahrain FinTech Ecosystem Report. *Bahrain FinTech Bay*. https://www.bahrainfintechbay.com/fintech-ecosystem-report

BFB. (2022). Bahrain FinTech Ecosystem Report 2022. *Bahrain FinTech Bay*.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS quarterly*, 17-32.

Boutin, C. (2023). *NIST Drafts Major Update to Its Widely Used Cybersecurity Framework*. NIST. https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

Brancato, G., Macchia, S., Murgia, M., Signore, M., Simeoni, G., Blanke, K., & Hoffmeyer-Zlotnik, J. (2006). Handbook of recommended practices for questionnaire development and testing in the European statistical system. *European Statistical System*.

Brock, J., Boltz, J., Doring, E., & Gilmore, M. (1999). Information security risk assessment practices of leading organizations. *Director, USGAO [online] http://www.gao.gov/special.pubs/ai00033.pdf (accessed 20 March 2009)*.

Brotby, K. (2009). *Information security governance: a practical development and implementation approach* (Vol. 53). John Wiley & Sons.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of research in Nursing*, *25*(8), 652-661.

Canelón, J., Huerta, E., Incera, J., & Ryan, T. (2019). A cybersecurity control framework for blockchain ecosystems. *International Journal of Digital Accounting Research*, *19*, 103-144.

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & Van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety–developing the conceptual framework. *Ergonomics*, *58*(4), 548-564.

Casoria, M. (2018). Cybersecurity as Enterprise Risk Within and Beyond the Bahraini Legal Framework. *KnE Engineering*, 37–51-37–51.

Cassidy McCants, J. B. (2023). 2023 identity theft statistics. https://www.consumeraffairs.com/finance/identity-theft-statistics.html

Castro, P., Rodrigues, J. P., & Teixeira, J. G. (2020). Understanding FinTech ecosystem evolution through service innovation and socio-technical system perspective. Exploring Service Science: 10th International Conference, IESS 2020, Porto, Portugal, February 5–7, 2020, Proceedings 10,

CBB. (2019). *Central Bank of Bahrain Rulebook Volume 1: Conventional Banks*. https://www.cbb.gov.bh/wp-content/uploads/2019/12/Final-OM-Enhancements-for-Cybersecurity-Vol-1.pdf

CBB, W. (2019). Central Bank of Bahrain | Home. https://www.cbb.gov.bh/

Clarke, V., & Braun, V. (2017). Commentary: Thematic analysis. *Journal of Positive Psychology*, *12*(3), 297-298.

Clegg, C. W. (2000). Sociotechnical principles for system design. *Applied ergonomics*, *31*(5), 463-477.

Clegg, C. W., Robinson, M. A., Davis, M. C., Bolton, L. E., Pieniazek, R. L., & McKay, A. (2017). Applying organizational psychology as a design science: A method for predicting malfunctions in socio-technical systems (PreMiSTS). *Design Science*, *3*, e6.

CNSSI. (2015). Committee on National Security Systems (CNSS) Glossary.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Davis, K., Maddock, R., & Foo, M. (2017). Catching up with Indonesia's fintech industry. *Law and Financial Markets Review*, *11*(1), 33-40.

Davis, M. C., Challenger, R., Jayewardene, D. N., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied ergonomics*, *45*(2), 171-180.

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, *2*(2), 25-36.

Didenko, A. (2020). Cybersecurity Regulation in Singapore's Financial Sector: Protecting FinTech 'Ants' in a Jungle Full of 'Elephants'. *UNSW Law Research*.

Didenko, A. N. (2020). Cybersecurity Regulation in Singapore's Financial Sector: Protecting FinTech 'Ants' in a Jungle Full of 'Elephants'. *UNSW Law Research Paper*(20-45).

Douglas, H. (2022). Sampling techniques for qualitative research. In *Principles of social research methodology* (pp. 415-426). Springer.

Egan, T. M., Yang, B., & Bartlett, K. R. (2004). The effects of organizational learning culture and job satisfaction on motivation to transfer learning and turnover intention. *Human resource development quarterly*, *15*(3), 279-301.

Ehrentraud, J., Ocampo, D. G., Garzoni, L., & Piccolo, M. (2020). Policy responses to fintech: a cross-country overview. *policycommons.net*, *FSI Insights No 23*.

Eickhoff, M., Muntermann, J., & Weinrich, T. (2017). What do FinTechs actually do? A taxonomy of FinTech business models.

Elnagdy, S. A., Qiu, M., & Gai, K. (2016). Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing. 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud),

ENISA. (2017). ENISA Overview of Cybersecurity and Related Terminology.

Eyal, I. (2017). Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*, *50*(9), 38-49.

Fadhul, S., & Hamdan, A. (2020). The Role of "FinTech" on Banking Performance. In (pp. 911-914,XVII). Reading: Academic Conferences International Limited.

Gai, K. (2014). A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. *Int. J. Comput. Appl*, *95*(3), 40-44.

Gai, K., Qiu, M., & Elnagdy, S. A. (2016). A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS),

Gai, K., Qiu, M., Sun, X., & Zhao, H. (2016). Security and privacy issues: A survey on FinTech. International Conference on Smart Computing and Communication,

Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, *87*(5), 537-580.

Gray, A., & Leibrock, M. (2017). Fintech and Financial Stability: Exploring How Technological Innovations Could Impact the Safety and Security of Global Markets. *DTCC Papers October*.

Group, W. B. (2018). *Financial Sector's Cybersecurity: Regulations and Supervision*. World Bank.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems*, *28*(2), 203-236.

Haddad, C., & Hornuf, L. (2019). The emergence of the global fintech market: economic and technological determinants. *Small Business Economics*, *53*(1), 81-105. https://doi.org/10.1007/s11187-018-9991-x

Hakmeh, J. (2018). Cybercrime Legislation in the GCC Countries. *International Security Department, Chatham House (The Royal Institute of International Affairs)*.

Harper, G. (2013). Mixed methods research. *Ipswich, MA: Salem Press Encyclopedia*.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

Hester, A. J. (2014). Socio-technical systems theory as a diagnostic tool for examining underutilization of wiki technology. *The Learning Organization*, *21*(1), 48-68.

Hu, Z., Ding, S., Li, S., Chen, L., & Yang, S. (2019). Adoption intention of fintech services for bank users: An empirical examination with an extended technology acceptance model. *Symmetry*, *11*(3), Article 340. https://doi.org/10.3390/sym11030340

Huang, R. H. (2018). Online P2P lending and regulatory responses in China: opportunities and challenges. *European Business Organization Law Review*, *19*(1), 63-92.

Hung, J. L., & Luo, B. (2016). FinTech in Taiwan: a case study of a Bank's strategic planning for an investment in a FinTech company. *Financial Innovation*, *2*(1), Article 15. https://doi.org/10.1186/s40854-016-0037-6

IBM_Security. (2023). *Cost of a Data Breach Report 2023*. I. Security.

iGA. (2019). *Information & eGovernment Authority*. http://www.iga.gov.bh/

ISACA. (2016). Cybersecurity Fundamentals Glossary, .

Kabanda, G. (2018). A cybersecurity culture framework and its impact on zimbabwean organizations. *Asian Journal of Management, Engineering & Computer Science*, *3*(4), 17-34.

Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Policy and Strategy Management in FinTech. In *Understanding Cybersecurity Management in FinTech* (pp. 153-166). Springer.

Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Policy and Strategy Management in FinTech. *Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends*, 153-166.

Keenan, M. (2015). Research methods. In: Salem Press Encyclopedia.

Kelly, S. E., Moher, D., & Clifford, T. J. (2016). Defining rapid reviews: a modified Delphi consensus approach. *International journal of technology assessment in health care*, *32*(4), 265-275.

Khaleej-Times, N. (2020). Over 50m cyber attacks recorded in GCC. *Khaleej Times Newspaper*. https://www.khaleejtimes.com/business/local/over-50m-cyber-attacks-recorded-in-gcc

Knapp, K. J. (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions: Threat Analysis and Response Solutions*. IGI Global.

Knewtson, H. S., & Rosenbaum, Z. A. (2020). Toward understanding FinTech and its industry. *Managerial Finance*.

Koffi, H. W. S. (2016). The Fintech Revolution: An Opportunity for the West African Financial Sector. *Open Journal of Applied Sciences*, *6*(11), 771-782.

Krueger, R. A. (2014). *Focus groups: A practical guide for applied research*. Sage publications.

LeCompte, M. D. (2000). Analyzing qualitative data. *Theory into practice*, *39*(3), 146-154.

Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School psychology quarterly*, *22*(4), 557.

Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School psychology quarterly*, *26*(1), 70.

Leong, K., & Sung, A. (2018). FinTech (Financial Technology): what is it and how to use technologies to create business value in fintech way? *International Journal of Innovation, Management and Technology*, *9*(2), 74-78.

Li, Y., Dai, W., Ming, Z., & Qiu, M. (2015). Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, *65*(5), 1339-1350.

Li, Z., Li, W., Wen, Q., Chen, J., Yin, W., & Liang, K. (2019). An efficient blind filter: Location privacy protection and the access control in FinTech. *Future Generation Computer Systems*, *100*, 797-810.

Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, *10*(6), 702-715.

Linstone, H. A., & Turoff, M. (1975). *The delphi method*. Addison-Wesley Reading, MA.

Magnuson, W. (2018). Regulating fintech. *Vanderbilt Law Review*, *71*(4), 1167-1226.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*.

Mawgoud, A. A., Taha, M. H. N., Khalifa, N. E. M., & Loey, M. (2019). Cyber security risks in MENA region: threats, challenges and countermeasures. International Conference on Advanced Intelligent Systems and Informatics,

Mbanaso, U. M., Abrahams, L., & Okafor, K. C. (2023). Research Philosophy, Design and Methodology. In U. M. Mbanaso, L. Abrahams, & K. C. Okafor (Eds.), *Research Techniques for Computer Science, Information Systems and Cybersecurity* (pp. 81-113). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-30031-8_6

McEvoy, T. R., & Kowalski, S. J. (2019). Deriving cyber security risks from human and organizational factors–a socio-technical approach. *Complex Systems Informatics and Modeling Quarterly*(18), 47-64.

McKinnel, D. R., Dargahi, T., Dehghantanha, A., & Choo, K.-K. R. (2019). A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Computers & Electrical Engineering*, *75*, 175-188.

Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., Kiah, M. M., Abbas, F., Hassan, M., & Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, *8*, 23391-23406.

Mehrotra, A. (2019). Financial Inclusion Through FinTech–A Case of Lost Focus. 2019 International Conference on Automation, Computational and Technology Management (ICACTM),

Miles, M. B., & Huberman, A. M. (1984). Qualitative data analysis: A sourcebook of new methods. In *Qualitative data analysis: a sourcebook of new methods* (pp. 263-263).

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Int J Surg*, *8*(5), 336-341.

Mulligan, S. P., Freeman, W. C., & Linebaugh, C. D. (2019). Data protection law: An overview. *Congressional Research Service*, *45631*, 25.

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information systems journal*, *16*(4), 317-342.

Najaf, K., Schinckus, C., & Yoong, L. C. (2020). VaR and market value of fintech companies: an analysis and evidence from global data. *Managerial Finance*, *47*(7), 915-936.

Ni, J., Yu, Y., Mu, Y., & Xia, Q. (2013). On the security of an efficient dynamic auditing protocol in cloud storage. *IEEE Transactions on Parallel and Distributed Systems*, *25*(10), 2760-2761.

NIST Kissel, R. (2011). *Glossary of key information security terms*. Diane Publishing.

Nomakuchi, T. (2018). A case study on fintech in Japan based on keystone strategy. 2018 Portland International Conference on Management of Engineering and Technology (PICMET),

Nussbaumer, P., Matter, I., & Schwabe, G. (2012). “Enforced” vs.“Casual” Transparency--Findings from IT-Supported Financial Advisory Encounters. *ACM Transactions on Management Information Systems (TMIS)*, *3*(2), 1-19.

O. Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and evolution*, *9*(1), 20-32.

Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching information systems and computing*. Sage.

Oosthuizen, R., & Pretorius, L. (2016). Assessing the impact of new technology on complex sociotechnical systems. *South African Journal of Industrial Engineering*, *27*(2), 15-29.

Overy, A. (2018). The Challenge Faced by all Those in the FinTech Market is How to Capture Innovation While Preserving the Stability of the Banking Network. *www.allenovery.com*.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, *372*.

Panetta, F. (2018). Fintech and banking: today and tomorrow. *Speech of the Deputy Governor of the Bank of Italy, Rome, 12th May*.

Parfitt, B. A. (1996). Using Spradley: an ethnosemantic approach to research. *Journal of Advanced Nursing*, *24*(2), 341-349.

Patten, M. L. (2016). *Understanding research methods: An overview of the essentials*. Routledge.

Petrosyan, A. (2023). *Global number of cyber attacks in financial sector 2013-2022*. Statista. https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/#statisticContainer

Project, F. (2022). Timeline of Cyber Incidents Involving Financial Institutions. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Rahman, S. A., Tuckerman, L., Vorley, T., & Gherhes, C. (2021). Resilient research in the field: Insights and lessons from adapting qualitative research projects during the COVID-19 pandemic. *International journal of qualitative methods*, *20*, 16094069211016106.

Raza Rabbani, M., Bashar, A., & Khan, S. (2021). Agility and Fintech is the Future of Islamic Finance: A Study from Islamic Banks in Bahrain. *Available at SSRN 3783171*.

Razzaque, A., Cummings, R. T., Karolak, M., & Hamdan, A. (2020). The propensity to use FinTech: input from bankers in the Kingdom of Bahrain. *Journal of Information & Knowledge Management*, *19*(01), 2040025.

Ropohl, G. (1999). Philosophy of socio-technical systems. *Society for Philosophy and Technology Quarterly Electronic Journal*, *4*(3), 186-194.

Rovai, A. P., Baker, J. D., & Ponton, M. K. (2013). *Social science research design and statistics: A practitioner's guide to research methods and IBM SPSS*. Watertree Press LLC.

Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International journal of forecasting*, *15*(4), 353-375.

Sachdeva, J. K. (2019). Business Research Methodology. . *Chennai: Himalaya Publishing House*

Sánchez, R., Almenares, F., Arias, P., Díaz-Sánchez, D., & Marín, A. (2012). Enhancing privacy and dynamic federation in IdM for consumer cloud computing. *IEEE Transactions on Consumer Electronics*, *58*(1), 95-103.

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for business students (Seventh). *Nueva York: Pearson Education*.

Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, *9*(3), 209-216. https://doi.org/10.1016/j.elerap.2009.07.005

Schilirò, D. (2021). Fintech in Dubai: Development and Ecosystem. *International Business Research*, *14*(11), 1-61.

Schlarman, S. (2007). Selecting an IT control framework. *EDPAC: The EDP Audit, Control, and Security Newsletter*, *35*(2), 11-17.

Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques. *decision Sciences*, *28*(3), 763-774.

Schryen, G., Wagner, G., & Benlian, A. (2015). Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of IS literature.

Schueffel, P. (2016). Taming the beast: A scientific definition of fintech. *Journal of Innovation Management*, *4*(4), 32-54.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer*, *10*(4), 16.

Shim, Y., & Shin, D. H. (2016). Analyzing China's Fintech Industry from the Perspective of Actor-Network Theory. *Telecommunications Policy*, *40*(2-3), 168-181. https://doi.org/10.1016/j.telpol.2015.11.005

Sipior, J. C., & Ward, B. T. (2008). A framework for information security management based on guiding standards: a United States perspective. *Issues in Informing Science and Information Technology*, *5*, 51-60.

Smith, W. (2019). *A comprehensive cybersecurity defense framework for large organizations* Nova Southeastern University].

Spradley, J. P. (1979). *The ethnographic interview*. Waveland Press.

Standardization, I. O. f. (2005). *Information Technology; Security Techniques; IT Network Security*. International Organization for Standardization.

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, *26*(1), 109-128. https://doi.org/10.1108/ICS-06-2017-0039

Suri, H. (2011). Purposeful Sampling in Qualitative Research Synthesis. *Qualitative Research Journal*, *11*(2), 63-75. https://doi.org/10.3316/QRJ1102063

Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (Fintech): a systematic literature review. *Information*, *11*(12), 590.

Susan, P., & Mykletun, R. J. (2014). Ageing workforce knowledge management and transactional & transformational leadership: A socio-technical systems framework and a Norwegian case study. *International Journal of Business and Social Science*, *5*(5).

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432.

Tellis, W. (1997). Introduction to case study. *The qualitative report*, *3*(2), 1-14.

Troyer, L. (2016). Expanding sociotechnical systems theory through the trans-disciplinary lens of complexity theory. *Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches*, 177-192.

Tsang, E. W. (2016). *The philosophy of management research*. Taylor & Francis.

Turcan, R. V., & Deák, B. (2021). Fintech–stick or carrot–in innovating and transforming a financial ecosystem: toward a typology of comfort zoning. *foresight*.

US_GAO. (1999). *Information Security Risk Assessment Practices of Leading Organizations*. U. G. A. O. GAO. https://www.gao.gov/assets/aimd-00-33.pdf

Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice*, *11*(2), 27-53.

Walker, G. H., Stanton, N. A., Jenkins, D., Salmon, P., Young, M., & Aujla, A. (2007). Sociotechnical theory and NEC system design. Engineering Psychology and Cognitive Ergonomics: 7th International Conference, EPCE 2007, Held as Part of HCI International 2007, Beijing, China, July 22-27, 2007. Proceedings 7,

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution. *MIS quarterly*, *39*(1), 91-112.

Whitworth, B. (2009). A brief introduction to sociotechnical systems. In *Encyclopedia of Information Science and Technology, Second Edition* (pp. 394-400). IGI Global.

Williams, C. (2007). Research methods. *Journal of Business & Economics Research (JBER)*, *5*(3).

Williamson, K. (2004). Research methods for students, academics and professionals: Information management and systems. *Library Review*.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering* (Vol. 236). Springer.

Wonglimpiyarat, J. (2017). FinTech banking industry: a systemic approach. *foresight*.

Zavolokina, L., Dolata, M., & Schwabe, G. (2016). FinTech transformation: How IT-enabled innovations shape the financial sector. FinanceCom 2016,

Appendices

8. Appendices

8.1. Appendix 1: Participant Information Sheet (PIS)

Project Title: Cybersecurity Framework for Bahrain's FinTech Stakeholders

1. An Invitation

I am conducting a research study in the area of a cybersecurity framework for FinTech entities in Bahrain. This is part of my PhD study at the University of Salford- UK. Prior to making a decision to participate, it is vital for you to understand the purpose of the research and the activities it will include. Please carefully review the following information before deciding if you want to participate. You are encouraged to discuss this research with others (if you like) prior to making your decision. If you have any questions or need further clarification, please let me know on my email: s.k.albenjasim@edu.salford.ac.uk.

2. What is the purpose of this research?

The winds of change are blowing across the financial systems, with services and advancements in Financial Technology (FinTech) influencing all aspects of the financial sector and generating a continual stream of innovations. Despite FinTech's advantages in efficiency improvement for financial services channels, competition enhancement, and financial inclusion promotion, it creates new challenges that endanger financial institutes' stability and integrity in general. Cyber-attacks such as (Phishing, Denial of Service, Malware, etc.), are used to threaten the security of FinTech. Therefore, cybersecurity is a concern to be addressed to manage risks properly while integrating FinTech electronic services.

This research will look into the definition of FinTech, highlight the challenges that FinTech faces, and find what measures can effectively manage FinTech cybersecurity risks. Furthermore, it provides an overview of the commonly adopted cybersecurity standards in the banking industry. The research will use these standards as the basis for proposing a cybersecurity framework for FinTech's stakeholders in Bahrain, as regulation for this subject is still recent. A framework that ensures an excellence level by creating a balance that optimises its advantages while lowering potential cyber threats to the financial system. Bahrain is used as a research field to illustrate the critical aspects involved in developing such a framework through in-depth research interviews of executives and business studies. This research endeavours to raise the level of cybersecurity and trusted electronic environment for both the customers and FinTech entities in Bahrain.

This research is part of the coursework for the Doctor of Philosophy that the researcher is undertaking. The results of the study will be analysed and published in the form of a doctoral thesis, and confidentiality of the participants and organisations will be strictly maintained.

3. How was I chosen for this invitation?

The researcher seeks to select professionals who work as cybersecurity experts, IT managers, executive directors, and IT auditors in financial organisations that have interacted with FinTech innovations. Since you come from one of the mentioned groups, it seemed appropriate to contact you for this purpose.

4. Do I have to take part?

The decision to take part is up to you. You will be provided with this information sheet if you want to take part, and you will be asked to sign the consent form. The participant will be given a copy of the information sheet and, if appropriate, a signed consent form to keep.

You may still withdraw at any time without affecting any benefits that you are entitled to in any way. You do not have to give a reason for withdrawing from the study.

However, if you do withdraw, the University may continue to analyse data or information you have already supplied. It will only do this for research purposes and in an anonymised way and in a way that you cannot be identified.

5. What will happen in this research?

The study analyses a significant number of previous studies on the rise of Financial Technology (FinTech) innovations and assesses the impact of cyber threats on these businesses. The results from previous research, along with newly gathered data, are used to identify the key principles of the cybersecurity framework for Bahrain’s FinTech stakeholders.

Primary data will be collected through research interviews with financial institute employees, executives, and FinTech experts in Bahrain.

The researcher formulates the research objectives and questions and decides on the data collection methods. For the Interviews, meetings will be scheduled with key stakeholders from banks and FinTech firms to discover deeper, transferable knowledge from field experts.

The gathered data will be analysed using descriptive statistics, and findings will be derived.

6. What are the discomforts and risks?

Since interviewing experts and getting their feedback on certain questions is an, there are no discomforts or risks.

7. What are the benefits?

This research endeavours to raise the level of cybersecurity and trusted electronic environment for both the customers and FinTech firms in Bahrain. The benefit for the participant in this research is that he will come to understand the key principles for an excellent cybersecurity framework that can be used as a guide for protecting FinTech firms from cyber-attacks. The researcher will get input on the critical aspects involved in developing such a framework through in-depth interviews with experts and business stakeholders.

8. How will my privacy be protected?

Your confidentiality and privacy will be maintained during and after the study. The names of the participants and/or the organisation will not be mentioned anywhere. Moreover, all the collected data will be stored securely by the following procedures:

a. Individual participant research data, such as interviews, will be anonymous and given a research code known only to the researcher and his supervisors (Research Team).

b. A master list identifying participants to the research codes data will be held on a password-protected computer accessed only by the researcher.

c. Hard paper/recorded (audio, photographic or video) data will be stored in a locked cabinet within a locked office, accessed only by the researcher.

d. Electronic data will be stored on a password-protected computer known only by the researcher.

e. The primary supervisors whose details have been provided at the end of this form will have access to view identifiable data for monitoring the research quality and study audit.

f. Collected Data is retained for as long as it is required to perform its purpose. At the end of that retention period, your data will either be deleted completely or anonymised.

9. Will I be recorded, and how will the recorded media be used?

The audio and/or video recordings of your activities made during this research will be used only for data collection and analysis. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings.

10. What are the costs of participating in this research?

The cost of participating is the time duration required for the interview. Depending on the size of the organisation and its cyber maturity, it may take around 60 minutes.

11. What opportunity do I have to consider this invitation?

The researcher would appreciate it if you could send a reply within two weeks of receiving this invitation.

12. How do I agree to participate in this research?

Once you agree to participate in the research, you may fill out a consent form that is given along with this sheet and send it to the researcher's email address that appeared on the form.

13. What will happen if I want to stop being part of the study?

If you decide to withdraw from the study, all the information and data collected from you to date will continue to be used; however, your name will be removed from all the study files.

14. Will I receive feedback on the results of this research?

If you so desire, you will be given a copy of the published result of the study. The results are scheduled to be released by the second quarter of the year 2024.

15. What do I do if I have concerns about this research?

If you have any questions or concerns about any aspect of this study, you should ask to speak to the researcher by email at s.k.albenjasim@edu.salford.ac.uk, who will do his best to answer your questions.

Alternatively, if you have any issues or complaints, you may contact the researcher's supervisors:

Dr Tooska Dargahi,– T.Dargahi@salford.ac.uk

Prof Haifa Takruri,– H.Takruri2@salford.ac.uk

16. Whom do I contact for further information about this research?

The researcher can be contacted for any details about the research. You may also contact the researcher's main supervisors, as listed above.

Contact Details:

Researcher’s name:

Salah AlBenJasim - s.k.albenjasim@edu.salford.ac.uk

Project Supervisor Contact Details:

Dr Tooska Dargahi,– T.Dargahi@salford.ac.uk

Prof Haifa Takruri,– H.Takruri2@salford.ac.uk

Thank you for your time in reviewing this information document.

8.2. Appendix 2: Interview Questions

Cybersecurity Framework for Bahrain's FinTech Entities Research Interview No. X

Section 1: Questions Related to General Characteristics Data

Financial Institute	
Business Name:	
Industry:	
No of Employees:	
Cybersecurity Standard adopted:	

Interviewee	
Name:	
Position Title:	
Main Roles:	
Qualifications:	
No of years at current business:	
Total Experience years:	

Section 2: Questions related to Cybersecurity Risk Assessment

Objectives	Questions
Cybersecurity Risk Assessment	1. What IT assets do you think are most vulnerable to cyber-attacks? 2. What are cyber threats targeting your organisation?

Section 3: Questions Related to Cybersecurity Policies and Governance

Objectives	Questions
Cybersecurity Policies and Governance	3. Which cybersecurity standards/framework your institution is committed to? a. What are the reasons for selecting this option? 4. Where do you think your company is in terms of the maturity of your Cybersecurity strategy? 5. Which regulatory/compliance issue(s) would be of concern if firms were to collaborate with other FinTech companies?

Section 4: Questions related to Level of Technology

Objectives	Questions
Level of Technology	6. What are the security technologies and solutions to protect against cyberattacks? 7. What types of security monitoring and protection tools are used for interpreting malicious activities? 8. What challenges do you face in implementing a cybersecurity protection solution?

Section 5: Questions related to Efficient CS operational processes.

Objectives	Questions
Efficient CS operational processes	9. What barriers inhibit your organisation from adequately defending against cyber threats?

Section 6: Questions related to Promoting Cybersecurity awareness and capacity building.

Objectives	Questions
Cybersecurity awareness and Capacity Building	10. What education, training, and awareness reinforcement are needed to improve end users' behaviours and workers' skills in the context of cybersecurity? 11. What are the most essential security skills required in your organisation?

Section 7: Questions related to the development of Cybersecurity Framework.

Questions
12. Should the government get more involved in helping to combat cyber threats in a systemically important industry like banking/financial services? 13. What measure makes a FinTech categorised as Excellence ranked within the cybersecurity maturity levels?

Date:	
Strat Time:	
Finish Time:	
Venue:	
Remarks:	

8.3. Appendix 3: Letter of Invitation

Dear ***participant's name***

It is a privilege to interact with you for the purpose of this study. I am a PhD student at the University of Salford's School of Science, Engineering & Environment, conducting empirical research as part of the Doctor of Philosophy degree requirements. The research title is: "Cybersecurity Framework for Bahrain's FinTech Stakeholders". I conduct interviews as part of this research to increase my understanding of how financial organisations are facing the new FinTech challenges from a cybersecurity perspective. As a ***participant's role*** specialist working at the ***participant's organisation*,** you are in an ideal position to give us valuable first-hand information from your viewpoint. Please keep in mind that your participation is entirely optional, and you may opt out at any moment.

The semi-structured interview lasts around one hour and is relatively informal. The interview questions are enclosed for your reference. Your feedback on the questions will be handled anonymously. To ensure that personal identification is not disclosed throughout the analysis and writing of results, each interview will be allocated a numerical code.

Your contribution will be beneficial to my research. The findings of this empirical study will be used to develop a cybersecurity framework for Bahraini FinTech stakeholders. The study results will be analysed and published as a PhD thesis, with the identity of the participants and organisations kept completely confidential.

Please suggest a day and time that suits you for participation, and I will make every effort to accommodate your schedule. Refer to the attached (PIS) document for details on the interviews. If you have any more questions, please don't hesitate to contact me at the email provided.

I appreciate your support.

Best Regards,

Salah AlBenJasim
PhD candidate
s.k.albenjasim@edu.salford.ac.uk

Dated:

8.4. Appendix 4: Consent Form

Research title: “Cybersecurity Framework for Bahrain’s FinTech Stakeholders”

Research Supervisors: Dr Tooska Dargahi, Prof Haifa Takruri

Researcher: Salah AlBenJasim

1. I confirm that I have reviewed the information sheet dated (*date*) for the research mentioned above. I have had the chance to review the information, raise questions, and receive satisfactory answers. □ Yes □ No
2. I acknowledge that my participation is optional, and I have the freedom to withdraw at any point without providing justification. □ Yes □ No
3. I understand that my data will be kept confidential and, if published, will not be identifiable as mine. □ Yes □ No
4. I agree that the interviews will be recorded and transcribed. □ Yes □ No
5. I consent to participate in this study. □ Yes □ No

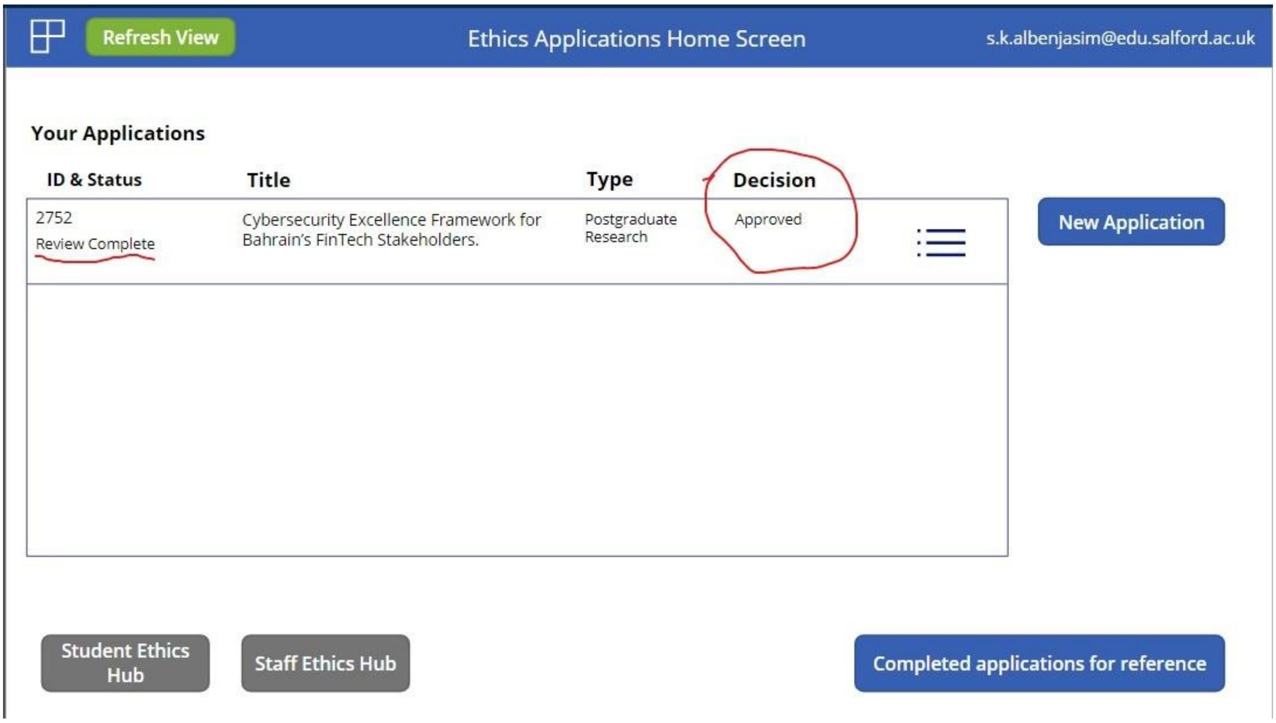
Participant

Signature:	
Name:	
Contact:	
Email:	
Date:	

Please provide me with the research findings: □ Yes □ No

Participant Reference: *xx*

8.5. Appendix 5: Ethics Approval



Ethics Applications Home Screen

s.k.albenjasim@edu.salford.ac.uk

Your Applications

ID & Status	Title	Type	Decision
2752 Review Complete	Cybersecurity Excellence Framework for Bahrain's FinTech Stakeholders.	Postgraduate Research	Approved

8.6. Appendix 6: Focus Group Survey

(Framework Review, Validation and Refining)

Personal Information	
Please include some personal information about your role and the firm for which you work. It is not required to input any personal or organisational information. This data will only be used to better understand and evaluate the findings.	
Education level	
Role	
Line of Business	
No of Employees	
No of experience Years	
Familiarity with cybersecurity standards/frameworks	
Survey Part 1 – Framework's Principles Validation	
Review the list of proposed principles for the CS framework. Add, delete or modify if needed. Review the definitions if possible.	

Principles	Definition	Comments/Feedback
Capacity Building and Awareness	The creation of dedicated cybersecurity curricula and awareness-raising programs, the expansion of training schemes and workforce-development programs, the adoption of international certification schemes, and the promotion of innovation and research are all examples of good practices.	
Regulation and Governance	Developing and maintaining regulatory standards that FinTech must follow; informing and assisting them in demonstrating compliance with the regulatory ecosystem; adapting regulations to the dynamic environment; using principle-based techniques; and controlling the protection of financial infrastructure in general.	
Risks Management	Internal controls and procedures that offer effective enterprise-wide risk management for protected service provision are used to ensure that the integrity of FinTech's services is protected and safeguarded.	
Secure Service Delivery	FinTech must understand the service delivery channels and infrastructure that connect customers to financial providers, as well as ensure that private information and transaction integrity are preserved. Maintaining the confidentiality of customer data, identifying customers, and guaranteeing their successful authentication throughout client	

	onboarding and transactions are all critical aspects of the secure delivery of FinTech services.	
Third Parties	Assuring that partners are committed via the proper channels without jeopardising the safety of FinTech's customers or its business.	
Best Practices	Ensure that FinTech service's security is maintained when new threats develop; ensure that regulatory bodies are aware of both current risks and their strategies to mitigate them; Audit on a regular basis and ensure that all reporting obligations are satisfied, among other things. Assuring that action is performed in collaboration with external partners, working with several national cybersecurity authorities, exchanging information about threats and events, and ensuring that FinTech firms have suitably trained human resources to deal with cyber threats.	
Add new if needed.		
General Feedback		
Your valuable insights and suggestions are welcomed.		

Survey Part 2 – Framework's Controls Validation

Review the list of proposed controls under each principle for the CS framework. Add, delete or modify if needed. Review the definitions if possible.

Principles	Controls		Comments/Feedback
Capacity Building and Awareness	Awareness Activities		
	Customers Protection		
	Human Resources		
	IT Staff training		
	Knowledge Mgt & Capacity Building		
Regulation and Governance	CBB Rule Books		
	Open Banking		
	Sandbox		
	Compliance		
	Management Support		
	Operational Processes		
	Event Log & Monitoring		
	Incident Management		
	Threat management		
	Strategy		
Risks Management	Assets		
	Data Protection		
	Review & Audit		
	Vulnerability Assessment		
Secure Service Delivery	Application Coding		
	Authentication		
	Encryption		
	Infrastructure		
Third Parties	Cloud Computing		
	Outsourcing		
	Vendor Support		
Best Practices	The road ahead		
	Collaboration		

	Maturity		
	Resilience		
Add new if needed.			
General Feedback			
Your valuable insights and suggestions are welcomed.			

8.7. Appendix 7: Delphi Rounds

Delphi Rounds Survey (Framework Refining and Ranking)

Personal Information	
Please include some personal information about your role and the firm for which you work. It is not required to input any personal or organisational information. This data will only be used to better understand and evaluate the findings.	
Education level	
Role	
Line of Business	
No of Employees	
No of experience Years	
Familiarity with cybersecurity standards/frameworks	

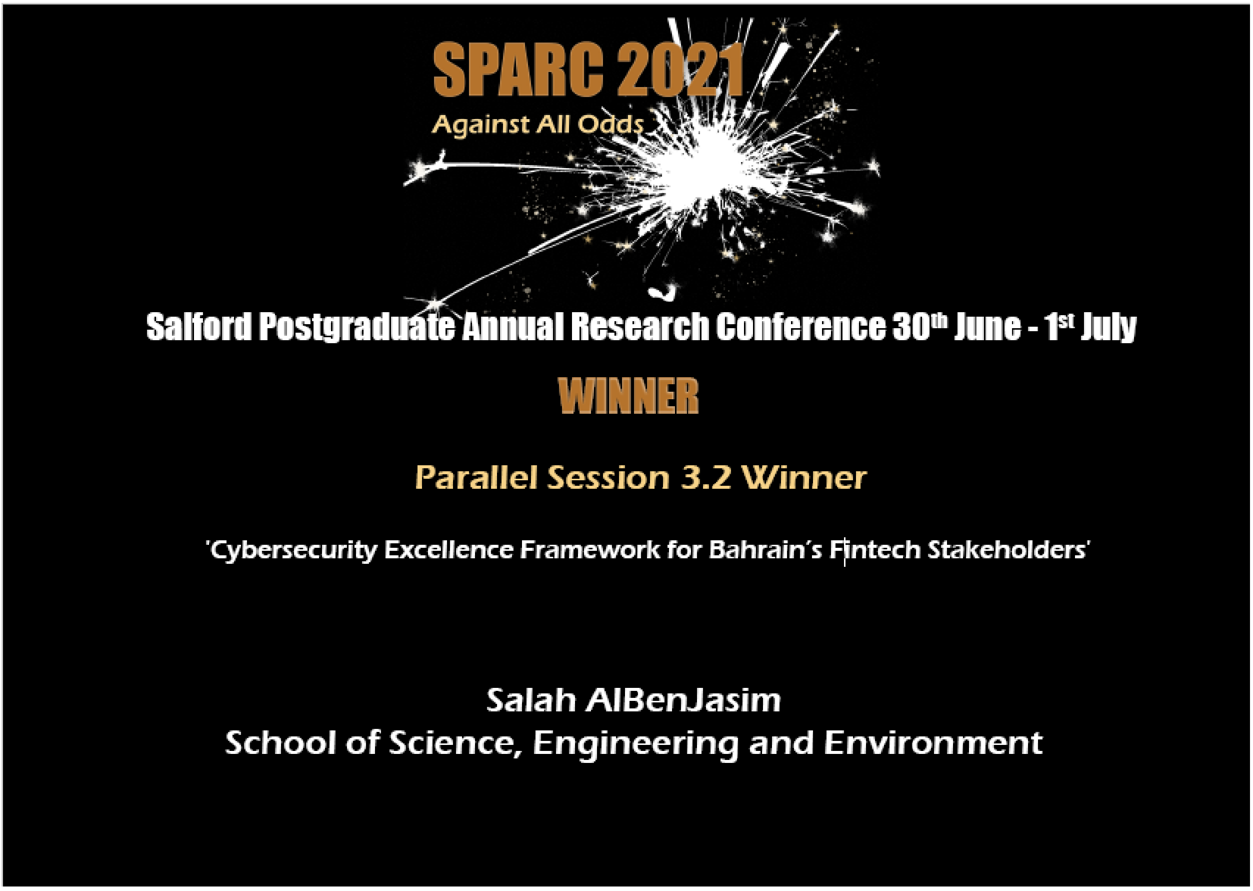
Survey Part 1 – Framework's Principles Refining and Ranking		
Principles	**Rank the principles :** **1 - Most Important** **6 - Least Important**	**Fill in the weight in % value totalling 100%**
	Rank (1-6)	**Weight (%)**
Capacity Building and Awareness		
Regulation and Governance		
Risks Management		
Secure Service Delivery		
Third Parties		
Best Practices		
Total		**100%**

General Feedback
Your valuable insights and suggestions are welcomed.

Survey Part 2 – Framework's Controls Refining and Ranking			
Principles	**Controls**	**Rank the controls** **1 - Most Important** **n - Lease Important**	**Fill in the weight in % value totalling 100%**
		Rank (1 most important)	**Weight (%)**
Capacity Building and Awareness	Awareness Activities		
	Communications		
	Management Support		
	IT Staff training		
	Knowledge Mgt & Capacity Building		
	Total		**100%**
Regulation and Governance	CBB Rule Books		
	Open Banking & Sandboxing		
	Compliance		
	CS Operational Processes		
	Strategy & Policy		
	Total		**100%**
Risks Management	Assets Management		
	Risk Mitigation		
	Review & Audit		
	Vulnerability Assessment		
	Total		**100%**
Secure Service Delivery	Application Coding		
	Authentication		
	Encryption		
	Secure Infrastructure		
	Total		**100%**
Third Parties	Cloud Computing		
	Outsourcing		
	Vendor Profile & Support		
	Total		**100%**
Best Practices	Future Scalability		
	Collaboration		
	Maturity		
	Resilience		
	Total		**100%**
General Feedback			
Your valuable insights and suggestions are welcomed.			

8.8. Appendix 8: Research Achievements

SPARC 2021 – WINNER SPEAKER



SPARC 2021

Against All Odds

Salford Postgraduate Annual Research Conference 30th June - 1st July

WINNER

Parallel Session 3.2 Winner

'Cybersecurity Excellence Framework for Bahrain's Fintech Stakeholders'

Salah AlBenJasim
School of Science, Engineering and Environment

SPARC – 2022 SEESION'S CHAIR AND SPEAKER

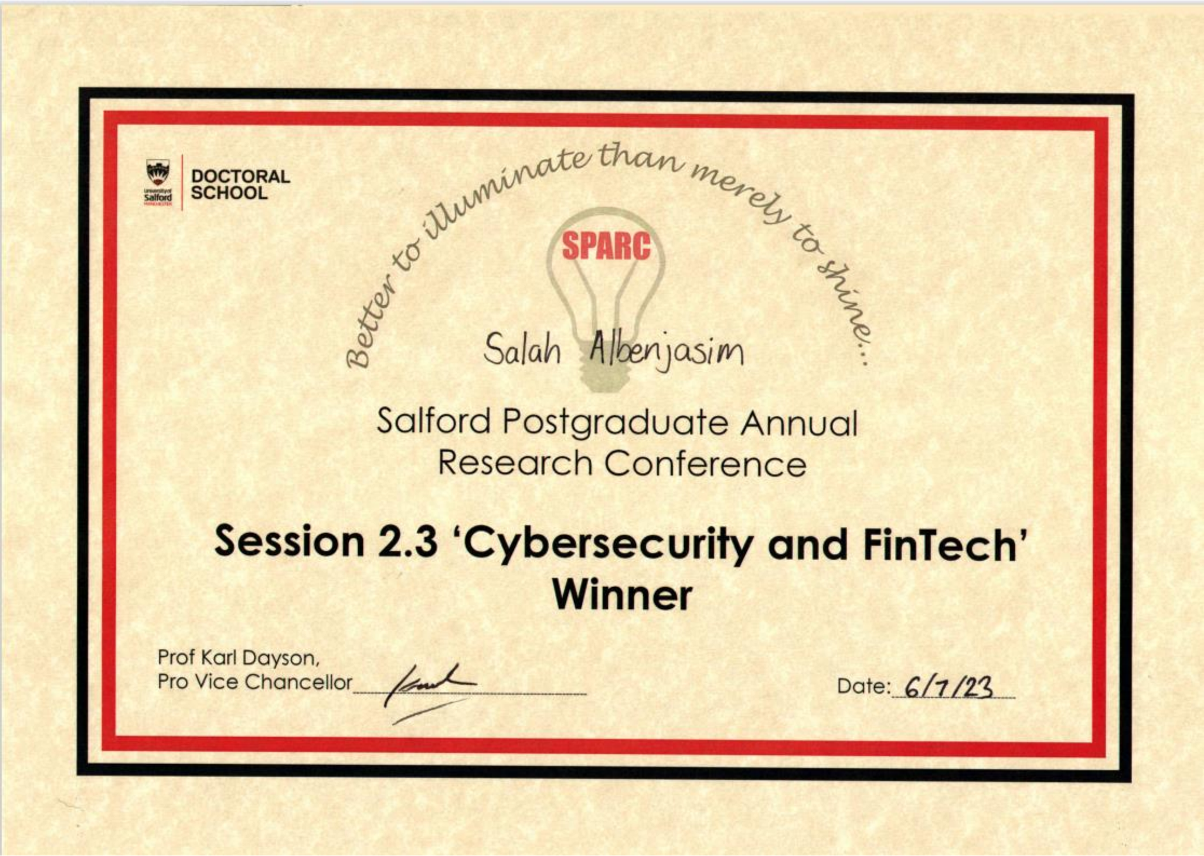
Day One, Wednesday 29th June 2022

Day 1 - 14.00 – 14.55 Parallel Session 2.2 Room 3.11	IMPROVING ENVIRONMENTS Chairs: **Salah AlBenJasim** and Dr Emma Smith A: **Lucy Barton**, ‘Prediction of Radiated Noise’ B: **Azreen Hamdan**, ‘Appraising The Criteria for Contractors’ Prequalification Processes for Building Construction Projects In Malaysia’ C: **Caster Martin**, ‘Comparing the Rheological Properties of Water-Based Mud Fluids Containing Nanoparticles Under High Pressure and High Temperature (HPHT) Conditions’ D: **Anisa Gumel**, ‘Analysis of Municipal Solid Waste Management in Nigeria’ E: **Anna Davison**, ‘Breaking Newt Ground: Detecting amphibians in a *Batrachochytrium salamandrivorans* infected area using environmental DNA.’

Day Two, Thursday 30th June 2022

Day 2 – 11.00 -11.55 Parallel Session 4.2 Room: 3.11	FINANCE AND CYBER SECURITY **Chairs:** Showbha B H Gowda and Prof Penny Cook A: **Perry Gonen**, ‘Investigation into the Co-integration of Foreign Direct Investment (FDI) and Startups in Israel’ B: **Nafisa Usman**, ‘FinTech and Money Laundering in Nigeria: Moderating Effect of Financial Regulations and Literacy’ C: **Ahmed Danladi Abdullahi**, ‘6G-Enabled Intelligent Transportation System, Security Challenges and Prospects: A Systematic Literature Review’ D: **Mohammed Yousif**, **‘**6G Network Communication, Architecture Core Network, Requirement, Security Issues and Key Challenge’ E: **Salah AlBenJasim**, ‘Development of Cybersecurity Framework for Bahrain’s FinTech Stakeholders’

SPARC 2023 – SESSION'S CHAIR AND WINNER SPEAKER



DOCTORAL SCHOOL

Better to illuminate than merely to shine...

SPARC

Salah Albenjasim

Salford Postgraduate Annual Research Conference

Session 2.3 'Cybersecurity and FinTech' Winner

Prof Karl Dayson,
Pro Vice Chancellor

Date: 6/7/23

PUBLISHED PAPER

Journal of Computer Information Systems

Salah AlBenJasim, Tooska Dargahi, Haifa Takruri & Rabab Al-Zaidi (2023): FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2023.2251455.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2023.2251455

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study

Salah AlBenJasim[a], Tooska Dargahi[b], Haifa Takruri[a], and Rabab Al-Zaidi[a]

[a]University of Salford, Manchester, UK; [b]Manchester Metropolitan University, Manchester, UK

ABSTRACT

Winds of change are blowing across the financial systems, with services and advancements in Financial Technology (FinTech) influencing all aspects of the financial sector and generating a continual stream of innovations. Despite benefits offered by FinTech, it creates new challenges that endanger financial institutes' stability and integrity. As cyber-attacks increasingly threaten the FinTech industry, cybersecurity can be considered as one of the main challenges that need to be addressed to properly manage risks associated with integrating FinTech services in people's day-to-day life. This Systematic Literature Review (SLR) highlights the cybersecurity challenges that FinTech industry faces and discusses existing measures that can effectively manage FinTech cybersecurity risks. An analysis of the existing literature and regulations is carried out to identify comparable components that exist across some internationally well-known cybersecurity standards and frameworks. Considering Bahrain as a case study, the paper explores key elements and factors that were not addressed adequately while implementing such standards. Research findings indicate that creating a cybersecurity framework for FinTech could be advantageous and offers a new perspective on the topic by demonstrating a natural extension of the existing knowledge. The findings offer useful suggestions for Bahrain's financial regulators to get better acquainted with these aspects. It lays the foundation to develop a cybersecurity framework for FinTech specifically for Bahrain, and it endeavors to raise the level of cybersecurity and a trusted electronic environment for both the customers and service providers in Bahrain.

KEYWORDS
Cybersecurity; FinTech; framework; Bahrain

Introduction

The advent of the Automated Teller Machine (ATM) was the most significant financial revolution in the banking sector. Previously, telegraphs were used to conduct financial transactions, which had been the case since 1838. To optimize its procedures, the banking sector utilized information technology to achieve this goal.[1] The rise of the Internet in the globe brought in a wave of technological innovations in a variety of fields. FinTech (Financial Technology) is a relatively new concept and innovative financial business that uses technology to enhance financial transactions.[2] FinTech is a new term referring to current interactions and, in particular, Internet-related technology (such as cloud computing and mobile Internet) and financial services sector operational processes (for example, lending money and banking transactions). FinTech represents a disturbance to the financial industry due to automated processes and the availability of Information and Communications Technology (ICT). In the financial services industry, FinTech offers a range of business models that integrate security, speed, and innovation.[3]

Based on the efforts of some international organizations and global standard setting entities, a modern conceptual model is developed as shown in Figure 1 and called the "FinTech Tree."[4]

FinTech tree differentiates between three categories, namely, FinTech activities, enabling technologies, and policy enablers. These activities are performed in various financial sectors and take different forms.

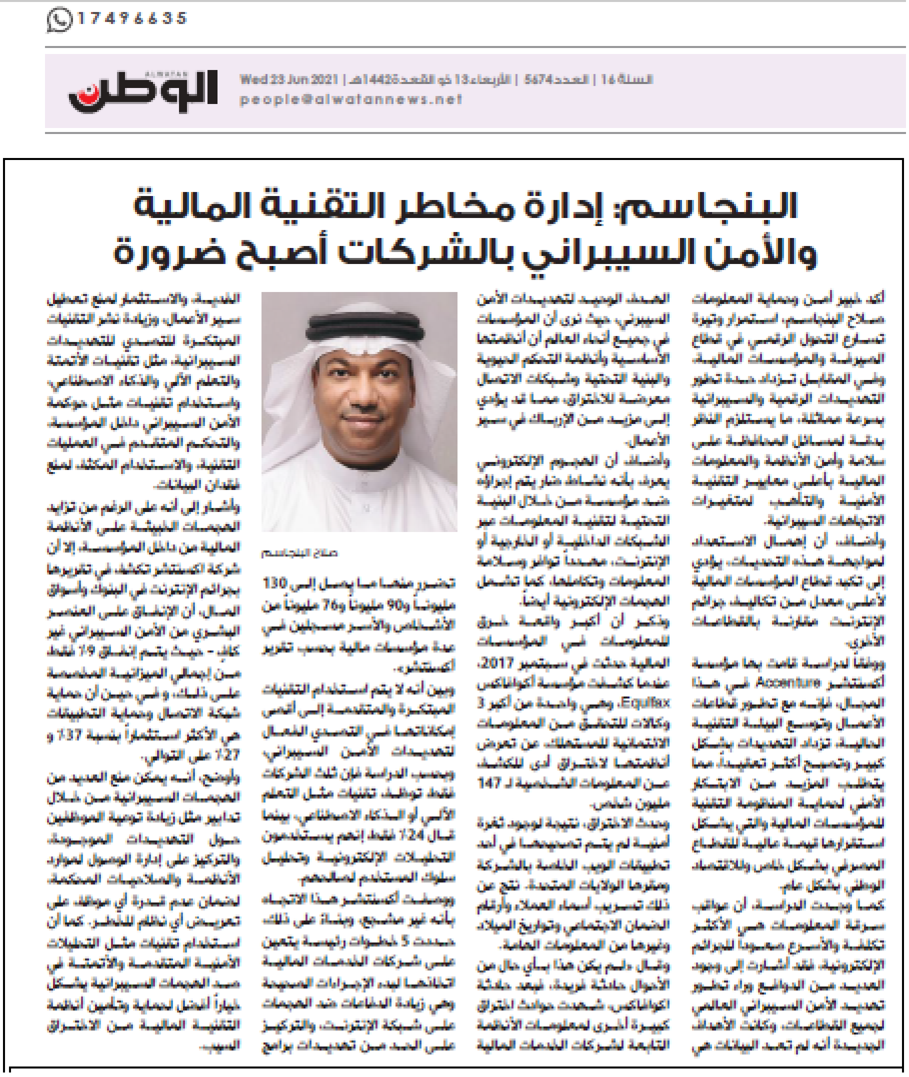
After the global financial crisis in 2008, advances in e-finance and mobile technologies for financial organizations fueled FinTech innovation. Integration in financial system innovation, Internet technology, social networking services, social media, artificial intelligence, cloud computing, and big data analytics characterized this evolution.

As the digital society widened, the actual risk of destructive cyber-attacks is constantly rising and puts pressure on all financial organizations to evolve and develop more viable cybersecurity protection measures.[5] Within FinTech contexts, cybersecurity plays a critical role in protecting businesses from losing their competitive edge. Indeed, today's vital financial systems are exposed to a variety of cyber threats that may disrupt the whole business model. In today's fast-paced environment, cybersecurity is anticipated to become an intrinsic element of the strategy, design,

Link to the paper:

https://doi.org/10.1080/08874417.2023.2251455

PUBLISHED ARTICLE IN BAHRAIN'S LOCAL NEWSPAPER – ARABIC



17496635

الوطن ALWATAN

السنة 16 | العدد 5674 | الأربعاء 13 ذو القعدة 1442هـ | Wed 23 Jun 2021
people@alwatannews.net

البنجاسم: إدارة مخاطر التقنية المالية والأمن السيبراني بالشركات أصبح ضرورة

أكد خبير أمن وحماية المعلومات صلاح البنجاسم، استمرار وتيرة تسارع التحول الرقمي في قطاع الصيرفة والمؤسسات المالية. وفي المقابل تزداد حدة تطور التهديدات الرقمية والسيبرانية بسرعة مماثلة، ما يستلزم النظر بدقة لمسائل المحافظة على سلامة وأمن الأنظمة والمعلومات المالية بأعلى معايير التقنية الأمنية والتأهب لمتغيرات الاتجاهات السيبرانية.

وأضاف، أن إهمال الاستعداد لمواجهة هذه التحديات، يؤدي إلى تكبد قطاع المؤسسات المالية لأعلى معدل من تكاليف جرائم الإنترنت مقارنة بالقطاعات الأخرى.

ووفقاً لدراسة قامت بها مؤسسة أكسنتشر Accenture في هذا المجال، فإنه مع تطور قطاعات الأعمال وتوسع البيئة التقنية المالية، تزداد التحديات بشكل كبير وتصبح أكثر تعقيداً، مما يتطلب المزيد من الابتكار الأمني لحماية المنظومة التقنية للمؤسسات المالية والتي يشكل استقرارها أهمية عالية للقطاع المصرفي بشكل خاص وللاقتصاد الوطني بشكل عام.

كما وجدت الدراسة أن عواقب سرقة المعلومات هي الأكثر تكلفة والأسرع صعوداً للجرائم الإلكترونية، فقد أشارت إلى وجود العديد من الدوافع وراء تطور تهديد الأمن السيبراني العالمي لجميع القطاعات، وكانت الأهداف الجديدة أنه لم تعد البيانات هي الهدف الوحيد لتهديدات الأمن السيبراني، حيث نرى أن المؤسسات في جميع أنحاء العالم أن أنظمتها الأساسية وأنظمة التحكم الحيوية والبنية التحتية وشبكات الاتصال معرضة للاختراق، مما قد يؤدي إلى مزيد من الإرباك في سير الأعمال.

وأضاف أن الهجوم الإلكتروني يعرف بأنه نشاط ضار يتم إجراؤه ضد مؤسسة من خلال البنية التحتية لتقنية المعلومات عبر الشبكات الداخلية أو الخارجية أو الإنترنت، مهدداً توافر وسلامة المعلومات وتكاملها، كما تشمل الهجمات الإلكترونية أيضاً.

وذكر أن أكبر واقعة خرق للمعلومات في المؤسسات المالية حدثت في سبتمبر 2017، عندما كشفت مؤسسة أكوافاكس Equifax، وهي واحدة من أكبر 3 وكالات للتحقق من المعلومات الائتمانية للمستهلك عن تعرض أنظمتها لاختراق أدى للكشف عن المعلومات الشخصية لـ 147 مليون شخص.

وحدث الاختراق، نتيجة لوجود ثغرة أمنية لم يتم تصحيحها في أحد تطبيقات الويب الخاصة بالشركة ومقرها الولايات المتحدة. نتج عن ذلك تسريب أسماء العملاء، وأرقام الضمان الاجتماعي وتواريخ الميلاد، وغيرها من المعلومات الخاصة.

وقال «لم يكن هذا بأي حال من الأحوال حادثة فريدة، فبعد حادثة أكوافاكس، شهدت حوادث اختراق كبيرة أخرى لمعلومات الأنظمة التابعة لشركات الخدمات المالية تخسر منها ما يصل إلى 130 مليوناً و90 مليوناً و76 مليوناً من الأشخاص والأسر مسجلين في عدة مؤسسات مالية بحسب تقرير أكسنتشر».

صلاح البنجاسم

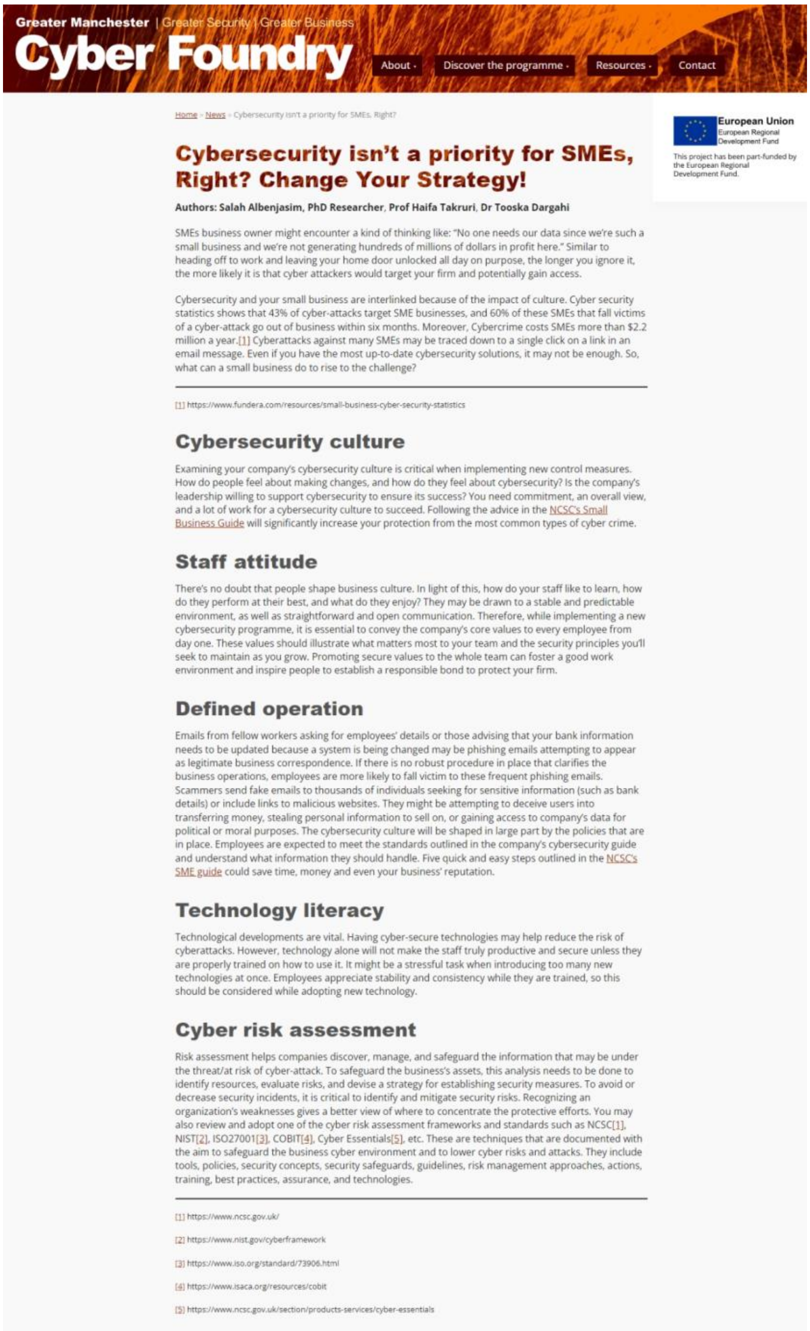
وبين أنه لا يتم استخدام التقنيات المبتكرة والمتقدمة إلى أقصى إمكاناتها في التصدي الفعال لتهديدات الأمن السيبراني. وبحسب الدراسة فإن ثلث الشركات فقط توظف تقنيات مثل التعلم الآلي أو الذكاء الاصطناعي، بينما قال 24٪ فقط إنهم يستخدمون التحليلات الإلكترونية وتحليل سلوك المستخدم لصالحهم.

ووصفت أكسنتشر هذا الاتجاه بأنه غير مشجع، وبناءً على ذلك حددت 5 خطوات رئيسة يتعين على شركات الخدمات المالية اتخاذها لبدء الإجراءات الصحيحة وهي زيادة الدفاعات ضد الهجمات على شبكة الإنترنت، والتركيز على الحد من تهديدات برامج الفدية، والاستثمار لمنع تعطيل سير الأعمال، وزيادة نشر التقنيات المبتكرة للتصدي للتهديدات السيبرانية، مثل تقنيات الأتمتة والتعلم الآلي والذكاء الاصطناعي، واستخدام تقنيات مثل حوكمة الأمن السيبراني داخل المؤسسة، والتحكم المتقدم في العمليات التقنية، والاستخدام المكثف لمنع فقدان البيانات.

وأشار إلى أنه على الرغم من تزايد الهجمات الخبيثة على الأنظمة المالية من داخل المؤسسة، إلا أن شركة أكسنتشر تكشف في تقريرها بجرائم الإنترنت في البنوك وأسواق المال، أن الإنفاق على العنصر البشري من الأمن السيبراني غير كاف - حيث يتم إنفاق 19٪ فقط من إجمالي الميزانية المخصصة على ذلك، وفي حين أن حماية شبكة الاتصال وحماية التطبيقات هي الأكثر استثماراً بنسبة 37٪ و 27٪ على التوالي.

وأوضح، أنه يمكن منع العديد من الهجمات السيبرانية من خلال تدابير مثل زيادة توعية الموظفين حول التهديدات الموجودة، والتركيز على إدارة الوصول لموارد الأنظمة والصلاحيات المحكمة لضمان عدم قدرة أي موظف على تعريض أي نظام للخطر، كما أن استخدام تقنيات مثل التحليلات الأمنية المتقدمة والأتمتة في صد الهجمات السيبرانية بشكل خياراً أفضل لحماية وتأمين أنظمة التقنية المالية من الاختراق السهل.

PUBLISHED ARTICLE IN GM CYBER FOUNDRY BLOG - ARTICLE 1


Greater Manchester | Greater Security | Greater Business
Cyber Foundry
About ·
Discover the programme ·
Resources ·
Contact
Home » News » Cybersecurity isn't a priority for SMEs, Right?
European Union
European Regional Development Fund
This project has been part-funded by the European Regional Development Fund.

Cybersecurity isn't a priority for SMEs, Right? Change Your Strategy!

Authors: Salah Albenjasim, PhD Researcher, Prof Haifa Takruri, Dr Tooska Dargahi

SMEs business owner might encounter a kind of thinking like: "No one needs our data since we're such a small business and we're not generating hundreds of millions of dollars in profit here." Similar to heading off to work and leaving your home door unlocked all day on purpose, the longer you ignore it, the more likely it is that cyber attackers would target your firm and potentially gain access.

Cybersecurity and your small business are interlinked because of the impact of culture. Cyber security statistics shows that 43% of cyber-attacks target SME businesses, and 60% of these SMEs that fall victims of a cyber-attack go out of business within six months. Moreover, Cybercrime costs SMEs more than $2.2 million a year.[1] Cyberattacks against many SMEs may be traced down to a single click on a link in an email message. Even if you have the most up-to-date cybersecurity solutions, it may not be enough. So, what can a small business do to rise to the challenge?

[1] https://www.fundera.com/resources/small-business-cyber-security-statistics

Cybersecurity culture

Examining your company's cybersecurity culture is critical when implementing new control measures. How do people feel about making changes, and how do they feel about cybersecurity? Is the company's leadership willing to support cybersecurity to ensure its success? You need commitment, an overall view, and a lot of work for a cybersecurity culture to succeed. Following the advice in the NCSC's Small Business Guide will significantly increase your protection from the most common types of cyber crime.

Staff attitude

There's no doubt that people shape business culture. In light of this, how do your staff like to learn, how do they perform at their best, and what do they enjoy? They may be drawn to a stable and predictable environment, as well as straightforward and open communication. Therefore, while implementing a new cybersecurity programme, it is essential to convey the company's core values to every employee from day one. These values should illustrate what matters most to your team and the security principles you'll seek to maintain as you grow. Promoting secure values to the whole team can foster a good work environment and inspire people to establish a responsible bond to protect your firm.

Defined operation

Emails from fellow workers asking for employees' details or those advising that your bank information needs to be updated because a system is being changed may be phishing emails attempting to appear as legitimate business correspondence. If there is no robust procedure in place that clarifies the business operations, employees are more likely to fall victim to these frequent phishing emails. Scammers send fake emails to thousands of individuals seeking for sensitive information (such as bank details) or include links to malicious websites. They might be attempting to deceive users into transferring money, stealing personal information to sell on, or gaining access to company's data for political or moral purposes. The cybersecurity culture will be shaped in large part by the policies that are in place. Employees are expected to meet the standards outlined in the company's cybersecurity guide and understand what information they should handle. Five quick and easy steps outlined in the NCSC's SME guide could save time, money and even your business' reputation.

Technology literacy

Technological developments are vital. Having cyber-secure technologies may help reduce the risk of cyberattacks. However, technology alone will not make the staff truly productive and secure unless they are properly trained on how to use it. It might be a stressful task when introducing too many new technologies at once. Employees appreciate stability and consistency while they are trained, so this should be considered while adopting new technology.

Cyber risk assessment

Risk assessment helps companies discover, manage, and safeguard the information that may be under the threat/at risk of cyber-attack. To safeguard the business's assets, this analysis needs to be done to identify resources, evaluate risks, and devise a strategy for establishing security measures. To avoid or decrease security incidents, it is critical to identify and mitigate security risks. Recognizing an organization's weaknesses gives a better view of where to concentrate the protective efforts. You may also review and adopt one of the cyber risk assessment frameworks and standards such as NCSC[1], NIST[2], ISO27001[3], COBIT[4], Cyber Essentials[5], etc. These are techniques that are documented with the aim to safeguard the business cyber environment and to lower cyber risks and attacks. They include tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies.

[1] https://www.ncsc.gov.uk/

[2] https://www.nist.gov/cyberframework

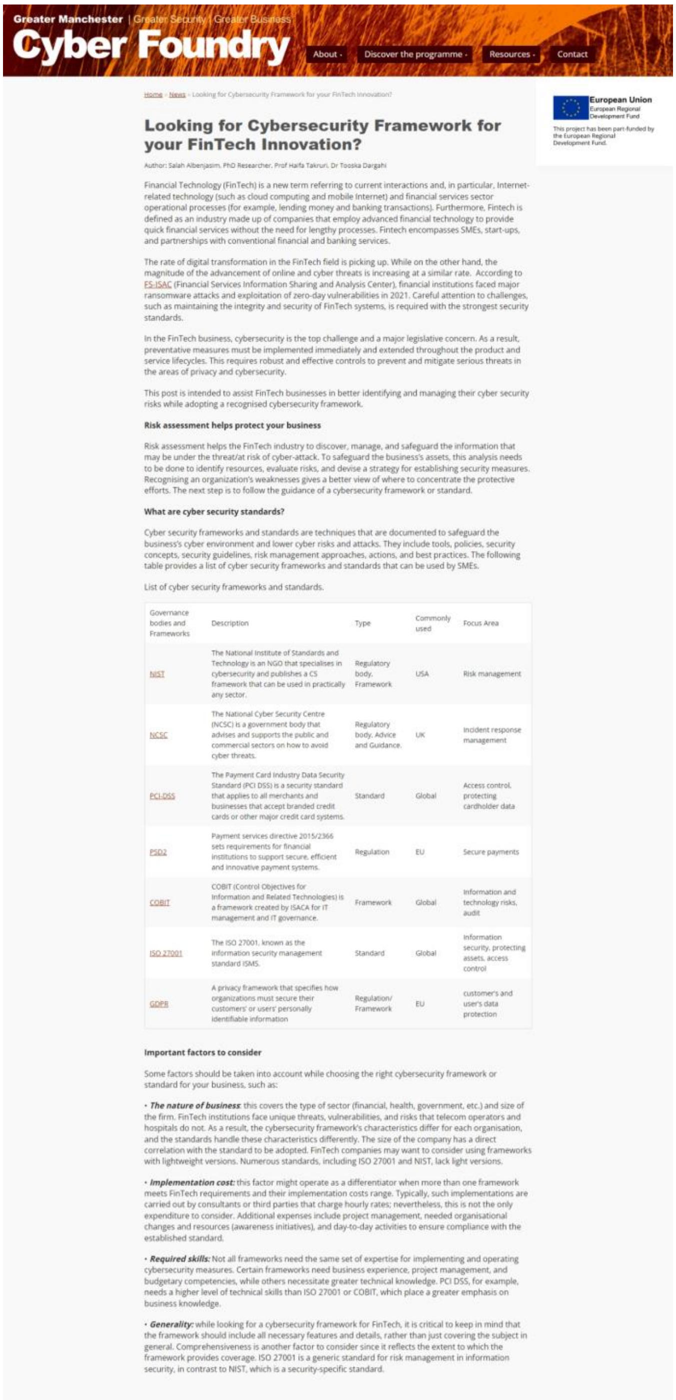
[3] https://www.iso.org/standard/73906.html

[4] https://www.isaca.org/resources/cobit

[5] https://www.ncsc.gov.uk/section/products-services/cyber-essentials

Cybersecurity isn't a priority for SMEs, Right? | gmcyberfoundry.ac.uk

PUBLISHED ARTICLE IN GM CYBER FOUNDRY BLOG - ARTICLE 2


Greater Manchester | Greater Security | Greater Business
Cyber Foundry
About
Discover the programme
Resources
Contact
European Union
European Regional Development Fund

Home › News › Looking for Cybersecurity Framework for your FinTech Innovation?

This project has been part-funded by the European Regional Development Fund.

Looking for Cybersecurity Framework for your FinTech Innovation?

Author: Salah Albenjasim, PhD Researcher, Prof Haifa Takruri, Dr Tooska Dargahi

Financial Technology (FinTech) is a new term referring to current interactions and, in particular, Internet-related technology (such as cloud computing and mobile Internet) and financial services sector operational processes (for example, lending money and banking transactions). Furthermore, Fintech is defined as an industry made up of companies that employ advanced financial technology to provide quick financial services without the need for lengthy processes. Fintech encompasses SMEs, start-ups, and partnerships with conventional financial and banking services.

The rate of digital transformation in the FinTech field is picking up. While on the other hand, the magnitude of the advancement of online and cyber threats is increasing at a similar rate. According to FS-ISAC (Financial Services Information Sharing and Analysis Center), financial institutions faced major ransomware attacks and exploitation of zero-day vulnerabilities in 2021. Careful attention to challenges, such as maintaining the integrity and security of FinTech systems, is required with the strongest security standards.

In the FinTech business, cybersecurity is the top challenge and a major legislative concern. As a result, preventative measures must be implemented immediately and extended throughout the product and service lifecycles. This requires robust and effective controls to prevent and mitigate serious threats in the areas of privacy and cybersecurity.

This post is intended to assist FinTech businesses in better identifying and managing their cyber security risks while adopting a recognised cybersecurity framework.

Risk assessment helps protect your business

Risk assessment helps the FinTech industry to discover, manage, and safeguard the information that may be under the threat/at risk of cyber-attack. To safeguard the business's assets, this analysis needs to be done to identify resources, evaluate risks, and devise a strategy for establishing security measures. Recognising an organization's weaknesses gives a better view of where to concentrate the protective efforts. The next step is to follow the guidance of a cybersecurity framework or standard.

What are cyber security standards?

Cyber security frameworks and standards are techniques that are documented to safeguard the business's cyber environment and lower cyber risks and attacks. They include tools, policies, security concepts, security guidelines, risk management approaches, actions, and best practices. The following table provides a list of cyber security frameworks and standards that can be used by SMEs.

List of cyber security frameworks and standards.

Governance bodies and Frameworks	Description	Type	Commonly used	Focus Area
NIST	The National Institute of Standards and Technology is an NGO that specialises in cybersecurity and publishes a CS framework that can be used in practically any sector.	Regulatory body, Framework	USA	Risk management
NCSC	The National Cyber Security Centre (NCSC) is a government body that advises and supports the public and commercial sectors on how to avoid cyber threats.	Regulatory body, Advice and Guidance.	UK	Incident response management
PCI-DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a security standard that applies to all merchants and businesses that accept branded credit cards or other major credit card systems.	Standard	Global	Access control, protecting cardholder data
PSD2	Payment services directive 2015/2366 sets requirements for financial institutions to support secure, efficient and innovative payment systems.	Regulation	EU	Secure payments
COBIT	COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for IT management and IT governance.	Framework	Global	Information and technology risks, audit
ISO 27001	The ISO 27001, known as the information security management standard ISMS.	Standard	Global	Information security, protecting assets, access control
GDPR	A privacy framework that specifies how organizations must secure their customers' or users' personally identifiable information	Regulation/ Framework	EU	customer's and user's data protection

Important factors to consider

Some factors should be taken into account while choosing the right cybersecurity framework or standard for your business, such as:

• ***The nature of business***: this covers the type of sector (financial, health, government, etc.) and size of the firm. FinTech institutions face unique threats, vulnerabilities, and risks that telecom operators and hospitals do not. As a result, the cybersecurity framework's characteristics differ for each organisation, and the standards handle these characteristics differently. The size of the company has a direct correlation with the standard to be adopted. FinTech companies may want to consider using frameworks with lightweight versions. Numerous standards, including ISO 27001 and NIST, lack light versions.

• ***Implementation cost:*** this factor might operate as a differentiator when more than one framework meets FinTech requirements and their implementation costs range. Typically, such implementations are carried out by consultants or third parties that charge hourly rates; nevertheless, this is not the only expenditure to consider. Additional expenses include project management, needed organisational changes and resources (awareness initiatives), and day-to-day activities to ensure compliance with the established standard.

• ***Required skills:*** Not all frameworks need the same set of expertise for implementing and operating cybersecurity measures. Certain frameworks need business experience, project management, and budgetary competencies, while others necessitate greater technical knowledge. PCI DSS, for example, needs a higher level of technical skills than ISO 27001 or COBIT, which place a greater emphasis on business knowledge.

• ***Generality:*** while looking for a cybersecurity framework for FinTech, it is critical to keep in mind that the framework should include all necessary features and details, rather than just covering the subject in general. Comprehensiveness is another factor to consider since it reflects the extent to which the framework provides coverage. ISO 27001 is a generic standard for risk management in information security, in contrast to NIST, which is a security-specific standard.

Are you looking for a Cybersecurity Framework for your FinTech Innovation? | gmcyberfoundry.ac.uk