International Cybersecurity Law Review
https://doi.org/10.1365/s43439-024-00130-4

ORIGINAL PAPER

Development of cybersecurity framework for FinTech innovations: Bahrain as a case study

Salah AlBenJasim · Haifa Takruri · Rabab Al-Zaidi · Tooska Dargahi

Received: 27 April 2024 / Accepted: 6 August 2024

Abstract FinTech is the term used to refer to financial and technology convergence space solutions. It usually refers to new innovations that conduct or connect with financial services via the internet, smart devices, software applications, or cloud services and encompasses anything from mobile banking to cryptocurrency applications. Despite the advantages of FinTech, 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, there is a notable gap in the literature regarding a focused cybersecurity framework that caters to the unique requirements of FinTech innovations, especially 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 an adaptable framework that addresses the risks and vulnerabilities faced by FinTech innovations in Bahrain.

Through panel discussions and Delphi sessions, industry experts evaluated the framework's practical feasibility, ability to address specific risks, and compatibility with the existing FinTech regulatory landscape. The results demonstrate a high

✉ Salah AlBenJasim · Haifa Takruri · Rabab Al-Zaidi
School of Science, Engineering & Environment, University of Salford, Salford, UK
E-Mail: S.K.Albenjasim@edu.salford.ac.uk

Tooska Dargahi
Computing and Mathematics Department, Manchester Metropolitan University, Manchester, UK

Published online: 13 September 2024

acceptance of the developed framework and highlight the framework's potential to enhance cybersecurity resilience significantly. Moreover, the experts acknowledge the proposed framework as a fundamental baseline in securing the FinTech ecosystem in Bahrain. The importance of this research lies in its potential to enhance the cybersecurity posture of the FinTech industry in Bahrain, mitigating risks and vulnerabilities associated with cyber threats in this vital sector.

Keywords Cybersecurity · FinTech · Framework · Bahrain

1 Introduction

Bahrain has a strategic plan keeping with the regional trend, which points out how its economy should diversify from oil. Vision 2030 was introduced in 2008 and relies on constructing 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 ICTs [1]. By achieving this, Bahrain's desire to become a hub for technology, innovation, and expertise could play a significant role in the region if the Gulf Cooperation Council (GCC) countries were to improve their economic cooperation.

In the past five years, to raise investment and economic growth, Bahrain has agreed to invest in FinTech's emerging trend [1]. 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, or products that have an associated contextual influence on financial markets and services provision. It provides a variety of advantages, in particular, improvements in performance and cost savings [2]. FinTech developments are also fundamentally changing the way people access financial services. At the same time, some of these innovations could also potentially threaten financial stability due to the disintermediation of regulated firms or activities.

However, the FinTech industry has become a prime target for cybercriminals due to the vast amounts of sensitive financial data they interact with. As a result, FinTech firms have been increasingly targeted by major cyber threat incidents in recent years. In 2021, a global survey [3] of financial institutions found that hackers increasingly preferred account takeovers as a method of attack. The report showed that attempted takeovers had risen by 282% between 2019 and 2020. While in 2022, there were a total of 1234 data breaches in the financial services industry. This represents a 10% increase from the previous year [4]. Moreover, the average data breach cost in the financial services industry is now $ 5.9 mio. This is significantly higher than the average cost of a data breach across all industries, which is $ 3.86 mio. [5].

While users have become more competent, attackers have also become more sophisticated. In fact, a significant 36% of data breaches are attributed to phishing attacks [6]. 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.

Table 1 *The state of Data breach in EMEA* [8]

Frequency	5379 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 Data Breach Investigations Report 2021 ([7]; Table 1) demonstrates the state of a data breach in Europe, the Middle East, and Africa (EMEA).

Trend Micro reported a combined 56,873,271 e-mails, URLs, malware, and banking malware attacks recorded in the Gulf Cooperation Council (GCC) region during the first half of 2020 [9]. 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 2294 banking malware incidences.

According to a cybersecurity market review report [10], In 2022, 42 companies in the GCC region fell prey to ransomware attacks. Of 42, 33% of companies were UAE-based, and 29% were from Saudi Arabia. A total of 21% of companies were reported from Kuwait and Qatar, whereas less than 10% of companies belonged to Oman and Bahrain.

1.1 Problem statement

The increasing number of cyberattacks specifically targeting FinTech companies necessitates that all financial organisations evolve and implement more effective cybersecurity measures [11]. A helpful countermeasure approach is to follow a cybersecurity standard, which acts as a collection of rules, policies, and procedures to handle cyber risks brought on by many highly advanced cyber threats. A cybersecurity framework strongly emphasises a scalable, adaptable, and economical method to stop cyber-attacks and boost the organisation's cyber resilience [12].

Although the topic of cybersecurity in the FinTech industry has gained considerable attention in recent years, current research on cybersecurity frameworks for the FinTech industry often adopts a broad approach. It neglects to account for the unique characteristics of the country's profile [11]. Moreover, there is a noticeable lack of research on developing a tailored cybersecurity framework, particularly for FinTech stakeholders. While there have been several studies on FinTech cybersecurity concerns in the broader Middle East area and worldwide, there is a shortage of research explicitly focusing on Bahrain's FinTech industry.

1.2 Research gap

The existing cybersecurity standards are primarily designed for conventional financial institutions or general technological settings. Nevertheless, the unique charac-

teristics of FinTech, such as the use of cutting-edge technology, cloud computing, open Application Programming Interfaces (APIs), and decentralised systems, demand a customised approach to promoting cybersecurity in this sector. FinTech entities, mainly start-ups, have adopted a rapid development cycle for their mobile application services before launching them to the market—which requires a more robust balance between growth speed and cybersecurity resiliency [13].

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, the dynamic nature of the FinTech industry, and the cybersecurity landscape. The current research studies may not sufficiently address the increasing risks and weaknesses distinct to the FinTech ecosystem.

Lastly, the attention given to assessing the efficacy of any proposed frameworks and consistently enhancing them over time is inadequate. Thus, effectiveness evaluation of the suggested framework is essential to identify any deficiencies or constraints and provide suggestions for improvements.

Considering Bahrain as a case study, this research provides an overview of the commonly adopted cybersecurity standards in the FinTech industry worldwide. It evaluates the missing gaps in Bahrain's FinTech context. The research addresses the problem by extensively reviewing existing cybersecurity challenges, common practices, and cybersecurity standards through in-depth research interviews with executives, experts, and other FinTech business stakeholders. Leveraging this knowledge, this research proposed an adaptable framework that addresses the risks and vulnerabilities faced by FinTech innovations 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.

1.3 Aim of the study

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 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. 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.

1.4 Significance of the research

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 contributes 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 can operate with increased confidence, knowing that their systems and data are protected. Furthermore, the results will benefit Bahrain's local stakeholders and provide significant insights and suggestions for other countries and areas with comparable FinTech ecosystems.

Following this introduction, a comprehensive analysis of existing literature related to the topic being studied is provided. Section 3 outlines the methodological approaches used: data collection and analysis procedures. Subsequently, Sect. 4 provides an in-depth review of the obtained findings, which will be further examined in Sect. 5. Section 6 discusses the framework validation exercise of the proposed framework. Finally, the study conclusions are given in the last Sect. 7.

2 Literature review

To address the research topic, it is essential to consider some literature, namely the cybersecurity challenges facing FinTech innovations and existing cybersecurity countermeasures, as outlined below. In recent years, various approaches for addressing cybersecurity challenges in FinTech have been established [14]. The findings of the literature review indicate that the constraints of FinTech research begin with identifying the FinTech framework [15, 16], which includes business models and models tailored to each organisation's culture. These factors have a significant impact on national regulations and policies [11, 14, 17, 18]. This sector necessitates conceptual frameworks that must be adjusted to technology advancements [14]. As a result, numerous countries have implemented the regulatory sandbox approach (FinTech start-up incubation), as seen in Singapore and Bahrain [19–22]. FinTech demands the collection of a lot of personal data. Therefore, it is vital to develop necessary measures for protecting consumer data [23]. The standard of data protection and infrastructure security must be regularly improved on this basis [12].

According to Addae et al. [24], cybersecurity controls may be categorised into three main types: technological countermeasures, operational countermeasures, and managerial countermeasures. These categories address the protection of confidentiality, integrity, and availability of a FinTech system. The primary goal of management and operational controls is on incidents and cybersecurity risks that people can manage and monitor, such as training, company-wide use policies, continuity planning, etc. Technical countermeasure is an approach to secure systems using technologically based solutions, such as intrusion detection systems, encryption technologies, and user authentication [25].

To harden FinTech's security, technologies such as biometry have been implemented in combination with tokenisation [26]. Furthermore, Public Key Infrastructure [27] and biometric-based authentication [28] have been introduced to strengthen the technical security controls of FinTech systems. Wang et al. [29] highlighted that antivirus software, intrusion detection systems, firewalls, and other perimeter and host-based countermeasures are inefficient in detecting and blocking insider attacks. According to Mawgoud et al. [30], some countermeasures and solutions are listed to tackle cyber risks for FinTech institutions, such as cyber surveillance, users' security awareness strategy, and legalisation setup.

FinTech businesses rely heavily on their information systems, so a well-structured framework would be essential to them. Part of the countermeasures is having a cybersecurity framework or standard that protects systems and mitigates cyber threats and vulnerability risks. Therefore, by following recognised cybersecurity frameworks, FinTech will most likely comply with regulations, often even before they become regulated.

2.1 Existing regulations

In our previous work, we analysed the existing literature and regulations to identify comparable components that exist across several internationally well-known cybersecurity standards and frameworks with a specific focus on Bahrain [8]. According to Al-Ahmad et al., standard certification does not always imply that FinTech is secure [31]. If not maintained appropriately, cybersecurity certifications might create an illusion of security. Additionally, since the standards are pretty system-oriented, excluding organisational factors, a comprehensive view of cybersecurity risk management is scarce. High implementation costs, a lack of qualified professionals, and the generality of standards extend to all the previously listed factors [31]. The generality of the standards does not account for variances in business risk needs, which might lead to different definitions by different stakeholders. Furthermore, the complexity of cybersecurity frameworks restricts their acceptance in particular businesses that lack the skills and resources to implement them [32]. To solve this issue, a light version is recommended that may be utilised as a starting point for many SMEs and FinTech companies. Businesses may also use it as a baseline for achieving a suitable degree of cybersecurity control and governance [31].

Cybersecurity in FinTech is a relatively new technology focus, so no dedicated cybersecurity framework exists for this field. However, there are some general cybersecurity frameworks and standards that regulators mandate businesses to follow to stay safe against cyber-attacks. These frameworks could be considered as a baseline for FinTech infrastructure protection. The systemic literature review by AlBenjasim et al. [8] provides a detailed list of the governance bodies and related components in each cybersecurity standard or framework.

These standards, frameworks and regulations 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 [12].

While numerous cybersecurity studies were conducted globally within the financial services sector, few types of research addressing the same field were undertaken in Bahrain. Our initial Systematic Literature Review (SLR) [8] in this domain served as a means to condense the current state of affairs within Bahrain's FinTech sector. Building on this groundwork, our present study aims to bridge the gap between academic research and its real-world implementation in the financial industry.

Benefiting from worldwide contributions, some studies seek to analyse current cybersecurity risk management standards, namely ISO 27001 [33]. 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 COBIT, PCI-DSS, and ISO 17799, as tools for regulatory fulfilment [34]. In this [35], the authors present a cybersecurity management framework that considers global, national, corporate, and personnel factors.

The more widespread FinTech innovations emerge, the more likely regulators will take action to guarantee that the information systems underlying these innovations are adequately protected and controlled. In the next section, we will further analyse the research gap and the need to develop a cybersecurity framework for FinTech specifically for Bahrain.

2.2 The need for cybersecurity framework for FinTech

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 strongly emphasises a scalable, adaptable, and economical method to stop cyber-attacks and boost the organisation's cyber resilience [12]. It is essential to understand that cybersecurity provides a financial institution with 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 [36–39]. A cybersecurity framework offers guidelines for monitoring cyber activities on the premises, designing preventive and detection methods, and taking necessary action to stop these activities 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 teams 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 [8]. The choice to invest in adopting a particular standard should be carefully evaluated [40]. 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 companies. We could not locate any research supporting adopting a certain standard as a curative for all cybersecurity risk challenges [8]. This is when a tailored approach may be the most excellent option. A customised approach leverages individual experience and transforms it into a solution that matches business needs. Rather than relying on the standards' prescribed elements, FinTech firms

might create their 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 [41]. A locally designed framework tends to grow and adapt over time while remaining closely aligned with FinTech business demands.

Thus, to investigate the critical aspects involved in developing such a framework for FinTech in Bahrain, this study will fulfil the below research question:

What are the crucial elements in developing a cybersecurity framework designed for FinTech entities in Bahrain? FinTech, in general, requires a robust cybersecurity framework to control both their business and technical operations. This research aims to develop a cybersecurity framework and common cybersecurity resources to support the FinTech sector against cyber threats. The framework aims to achieve excellence by striking a balance that maximises its benefits while minimising potential cyber risks to the financial system.

3 Research methodology

A qualitative methodology is used to meet the objectives of this study. Depending on the area of research, this technique may take many different types [42]. This method aims to have a broader understanding of the results collected and make evident conclusions. For the qualitative data, interviews were scheduled with crucial stakeholders from banks and FinTech firms in Bahrain to discover more profound, transferable knowledge from field experts. Cybersecurity Regulations published by the Central Bank of Bahrain for local financial institutes were reviewed and studied. The outcomes of such investigations will help design the research tool as interview questions to explore the critical aspects involved in developing a cybersecurity framework for FinTech in Bahrain.

To verify the theoretical cybersecurity controls, it is necessary to look at the methodological approaches while investigating the answer to the research question. It was determined that the research 'onion' approach created by Saunders, Lewis, and Thornhill [43] would be the best plan to use for this study. This has been used by a variety of researchers [44, 45] to gain an understanding of each step that comprises the research process. Many different research philosophies, strategies, options, methods, timeframes, tools, and processes for data gathering are the diverse layers that make up this onion.

This type of research mainly concentrates on actual practices by examining how businesses typically operate. According to Silverman, a case study design is suitable for researchers aiming to analyse an in-depth event, action, or process of a few people, making it the best design for addressing the research question [46]. Therefore, the study used an exploratory qualitative methodology to comprehend the circumstances or situations related to cybersecurity in Bahrain's financial sector. This helped us to carefully and meaningfully address the research question using qualitative data findings. Moreover, the qualitative method helped us define and evaluate the consis-

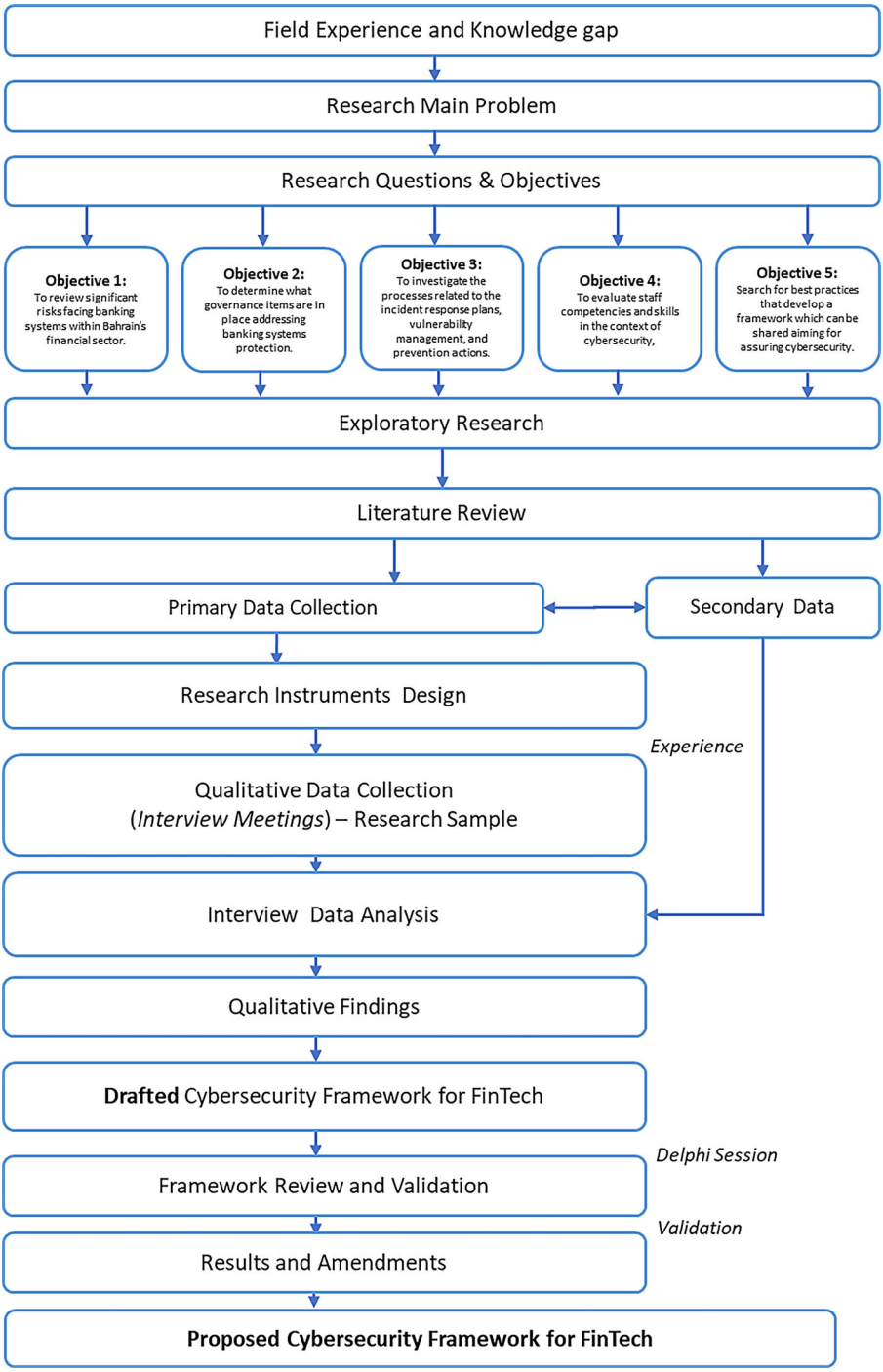

Fig. 1 Research Design and Plan

tency and correctness of the findings by comparing the data from various sources. Fig. 1 depicts the research design and plan.

4 Data collection & analysis

For the adopted qualitative methodology, in-depth research interviews were conducted with professionals who possess valuable expertise and insights in the FinTech domain. These include executives, experts, and other stakeholders intimately involved in Bahrain's 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.

4.1 Population of the study

The research population for this study comprises executive leaders, IT managers, risk, compliance, and legal specialists, cybersecurity auditors and consultants, and Information security and IT specialists who have a part in business operations, regulatory, or compliance activities inside Bahrain financial institutions. According to Suri [47], the research 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 [47]. Population is used as a means for identifying the whole from which the sample is selected [48]. These individuals will be interviewed for the purpose of data collection and are the target group for this qualitative research.

4.2 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 [43]. The determination of sample size in qualitative research is guided by the principle of data saturation [48]. 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 aims to find and gather information from instances that are rich and relevant to a given subject of interest or phenomena [47].

Qualitative research studies often use a very limited sample size, generally ranging from 12 to 20 people [49]. 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 2 shows the sampling groups contacted and those who responded and agreed to participate.

Table 2 Sampling Groups

Sampling Groups	Contacted	Agree to participate
Executive management	5	3
Business Owners & Managers	4	4
Compliance, risk, and law experts	2	1
IT Professionals and consultants	3	3
Cybersecurity Experts	4	2
Financial industry Regulator	2	1
Total	*20*	*14*

4.3 Interview questions

For the data collection, interviews were scheduled with the research sample group to get more profound and broader knowledge from operational and technical experts. The interviewees included various experts who cared about cybersecurity for FinTech.

Although there are only a few interview questions, these 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. Table 3 lists guided questions asked/discussed during the interviews.

4.4 Participants characteristics

Twenty Professionals who work as cybersecurity experts, IT managers, executive directors, and IT auditors interacting with FinTech innovations were contacted formally to get their agreement to participate in the study. 14 participants agreed to be

Table 3 Interview Questions

Interview Questions	
1.	What IT assets do you think are most vulnerable to cyber-attacks? What are cyber threats targeting your organisation?
2.	Which cybersecurity standards/frameworks your institution is committed to? What are the reasons for selecting them?
3.	Where do you think your company is in terms of the maturity of your Cybersecurity strategy?
4.	Which regulatory/compliance issue(s) would be of concern if firms collaborated with other FinTech companies?
5.	What are the security technologies and solutions to protect against cyberattacks?
6.	What security monitoring and protection tools are used to interpret malicious activities?
7.	What challenges do you face in implementing a cybersecurity protection solution?
8.	What barriers inhibit your organisation from adequately defending against cyber threats?
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 essential security skills required in your organisation?
10.	Should the government get more involved in helping to combat cyber threats in a systemically important industry like banking/financial services?

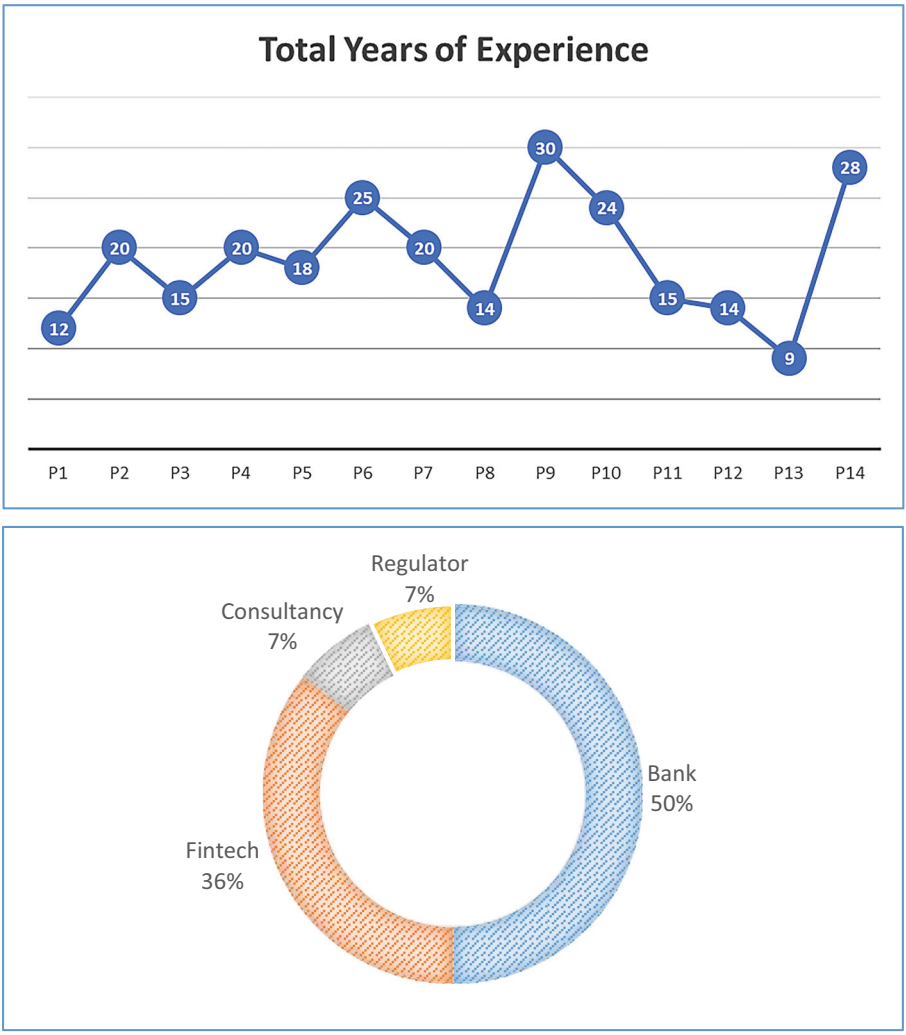

Fig. 2 Total years of experience for the participants and line of businesses

part of this study. Figure 2 shows the total years of experience for the participants and the line of businesses they are working with.

4.5 Interviews and data collection

All the interviews were conducted using MS Teams audioconferencing software, and the data was collected between January and April 2022. The 14 interviews lasted 763 min in total. Each interview lasted an average of 54 min.

At the end of each interview, MS Teams automatically transcribed the conversation. After that, many rounds of analysis were carried out. Each transcript was first-hand-coded and constituted a dataset inside the corresponding interview discussion.

The first set of codes was obtained from the research questions to guarantee that the analyses, themes, and supporting patterns were aligned with the research question. 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 imported into the latest version of NVivo software [50].

Another level of analysis using the NVivo program is performed, including pattern coding and classification. To fulfil the requirement of theme analysis, this extra analysis required looking for repeated patterns in all the data connected to the research question. The thematic analysis comprises the recursive investigation and evaluation of codes, themes, and patterns to establish their validity in relation to the data obtained [51]. This increased consistency assures quality and is an advantage of using the theme analysis technique.

4.6 Bahrain FinTech stakeholders

During interviews and discussions with the experts, FinTech services vary from traditional financial services in several ways. First is the customer domain, where services are 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 is drawn to serve as both a reference and a classifying scheme. The service model used in

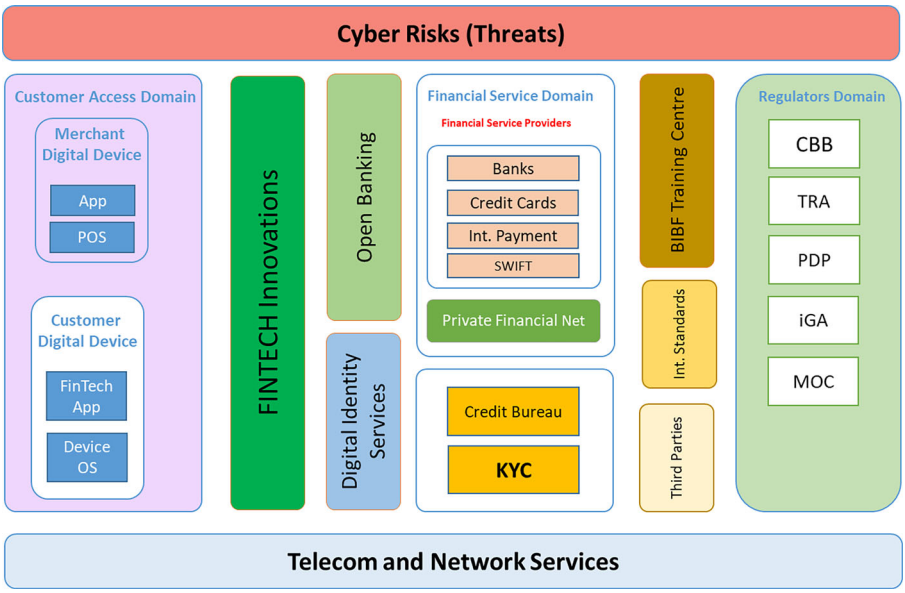

Fig. 3 Identified FinTech stakeholders in Bahrain

investigating cybersecurity threats for FinTech's stakeholders is shown in Fig. 3. The diagram depicts the wide variety of players engaged in the delivery of FinTech services and the many ways in which they are connected and interact. This will facilitate the comprehension of the relationships between customers, entities, agents, layers, and functions in Bahrain's financial sector. Moreover, it will establish a shared understanding of a FinTech ecosystem and the cyber threats and risks surrounding it.

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 particular 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.

Table 4 gives an overview and analytics of the concerns brought up by the experts regarding the FinTech business's cybersecurity environment. The participants

Table 4 Participants' Feedback and Highlights

Participants	Feedback and Highlights
P4, P6, P7	The existing regulatory guidance in Bahrain exhibited shortcomings in effectively addressing the dynamic landscape of cyber threats and the need to update cybersecurity guidelines for the FinTech sector regularly
P2, P9, P10, P11	There was a lack of attention given to the need for third-party risk management, particularly in evaluating and supervising the cybersecurity measures used by vendors and partners operating within the FinTech ecosystem
P4, P5, P8	Insufficient consideration was given to the unique challenges and threats inherent to the FinTech sector while adopting cybersecurity standards. These issues include the incorporation of emerging technologies like blockchain or mobile payments
P1, P8, P9, P14	Inadequate clarity and advice on incident response and recovery protocols associated with FinTech were observed, highlighting the significance of these procedures in mitigating the consequences of cyber incidents and maintaining uninterrupted business operations
P1, P2, P6, P12, P13, P14	Establishing a unified and effective cybersecurity ecosystem became difficult due to the lack of attention given to the coordination and cooperation among regulatory agencies, financial institutions, national government, and technology partners
All	Not enough focus was devoted to the significance of cybersecurity awareness and training activities for personnel in FinTech businesses, resulting in a possible deficiency in human-centric security measures
P1, P2, P3, P4, P5, P11, P13, P14	Implementing and enforcing comprehensive data privacy and protection measures, particularly regarding the sensitive financial information managed by FinTech companies, were inadequate
P3, P4, P5, P7, P12, P13	The consistent enforcement of assessment and systems integrity procedures for the cybersecurity posture of FinTech entities, such as frequent audits and penetration testing, was lacking, resulting in the possibility of undiscovered vulnerabilities
P3, P5, P6, P8, P10, P12	The significance of particularly secure software development practices, including secure coding standards and comprehensive testing, was not adequately stressed, potentially leading to vulnerabilities in FinTech applications
All	The absence of a comprehensive structure for incident reporting and information sharing within the FinTech industry has negatively impacted the sector's capacity to address new threats and vulnerabilities promptly

identified several areas that need improvement to address how cyber threats are growing and to build a robust cybersecurity ecosystem. The common concerns of the experts are the regulatory structure, third-party risk management, taking unique challenges into account, handling incidents procedures, coordination and collaboration, cybersecurity awareness, data protection, cybersecurity assessment, secure software development, and reporting of incidents.

5 Thematic analysis & results

The data analysis is among the most crucial tasks in the qualitative research process [52]. The research philosophy and approach determine the methodologies utilised to analyse qualitative data. The process of eliminating enormous volumes of gathered data to make meaning of it is known as data analysis, composed of three steps: data is structured, data is condensed via summary and classification, and patterns and themes in the data are recognised and connected [53]. We were receptive to new elements revealed inductively via data analysis and were willing to adjust the components of the cybersecurity framework 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 [54].

To analyse qualitative data, a typical five-point approach, known as LeCompte's methodology in Fig. 4, drawn from [53], was adopted. Therefore, it would be easier to discover the factors influencing FinTech's cybersecurity controls by utilising the existing literature, data collected, and LeCompte's methodology. These theoretical assumptions may converge significantly to what the participants think.

5.1 Themes and supporting patterns

Using the above qualitative analysis methodology, this section presents the common themes and supporting patterns throughout the data collected by interviewing the sample groups. It focuses further on the research themes from collected data and

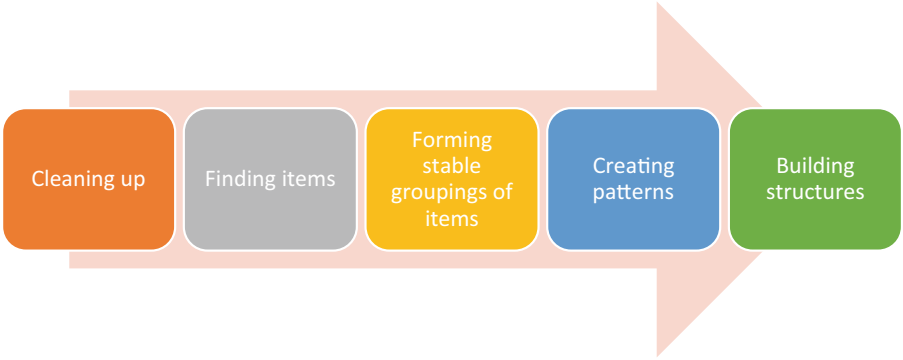

Fig. 4 Typical five-point approach drawn from LeCompte's [53]

	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%

Fig. 5 The common items extracted and the word count in terms of '% coverage'

describes the critical aspects of developing a cybersecurity framework for FinTech innovations in Bahrain.

5.1.1 Cleaning up

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

5.1.2 Finding items

The Nvivo software was used to import the transcribed interviews. Items emerge through repeated readings of the transcribed interviews to highlight topics relevant to the research questions (termed as codes in Nvivo). Figure 5 lists thirty-six items that commonly emerged from the 14 individuals' interview session analysis.

The results demonstrate that all the items included in the aspects relevant to the cybersecurity framework for FinTech were agreed upon by all the participants.

Fig. 6 Codes Word Cloud

We assume that the frequency of words and themes offers a decent indicator of meaningfulness, as [52] found word count beneficial. In this case, word count was utilised to determine and analyse the participants' attention in Fig. 7. The word count in terms of '% coverage' (Table 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 analysed text. Word clouds are becoming more popular as a simple technique to identify the focus of written material.

Figure 6 highlighted words like cyber, security, people, organisation, information, controls, risk, process, etc., as more frequent topics and areas during the interviews. Incorporating concepts from the theoretical framework discussed in the literature shows how people, processes, and technology interact in reference to the cybersecurity model for FinTech.

For instance, interviewees emphasised, as shown in Fig. 7, the significance of capacity building and awareness, as well as regulation and governance, as important topics to address cybersecurity controls for FinTech in Bahrain.

Based on the participants' answers, themes were developed. Nvivo was used to determine how often the items appeared by displaying their percentages in Table 4 to identify which topics the respondents paid the most attention to.

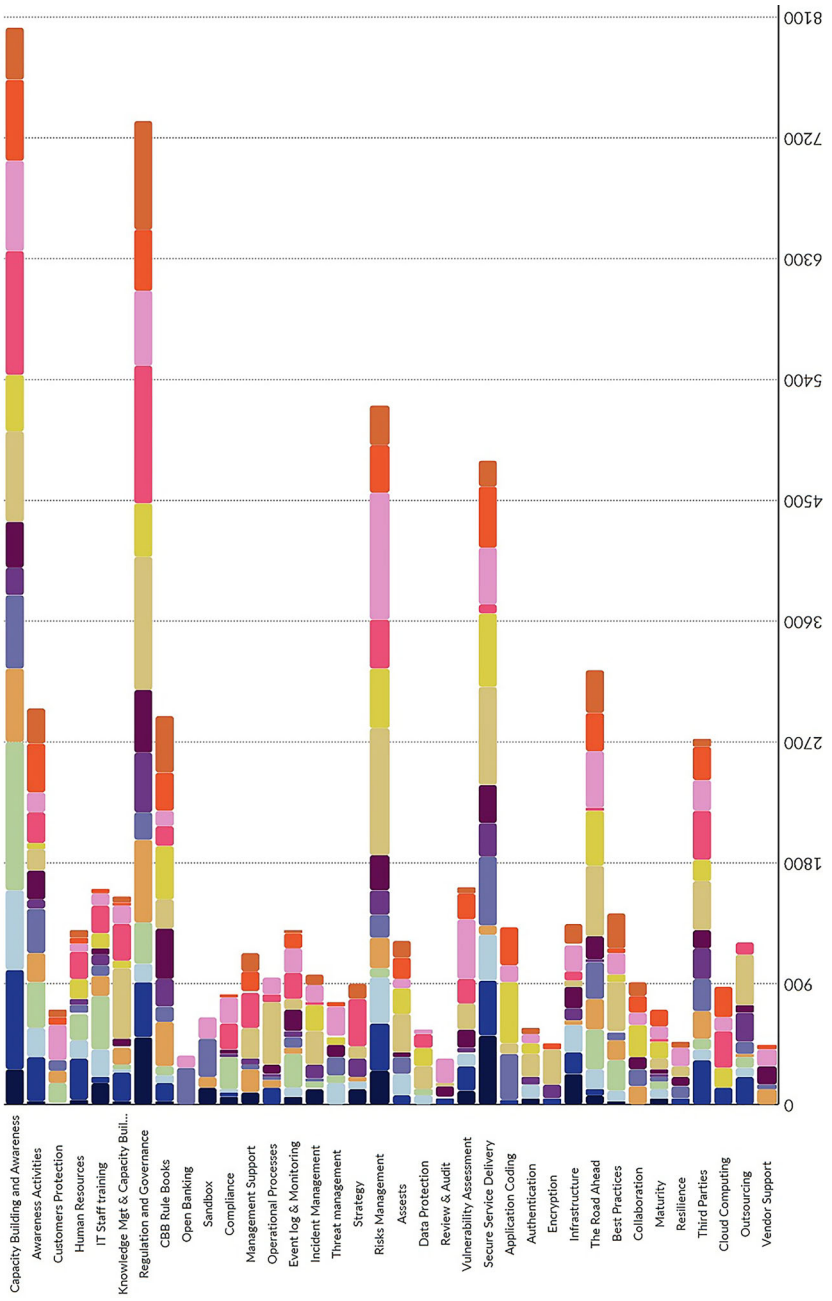

Fig. 7 Matrix Coding and word count

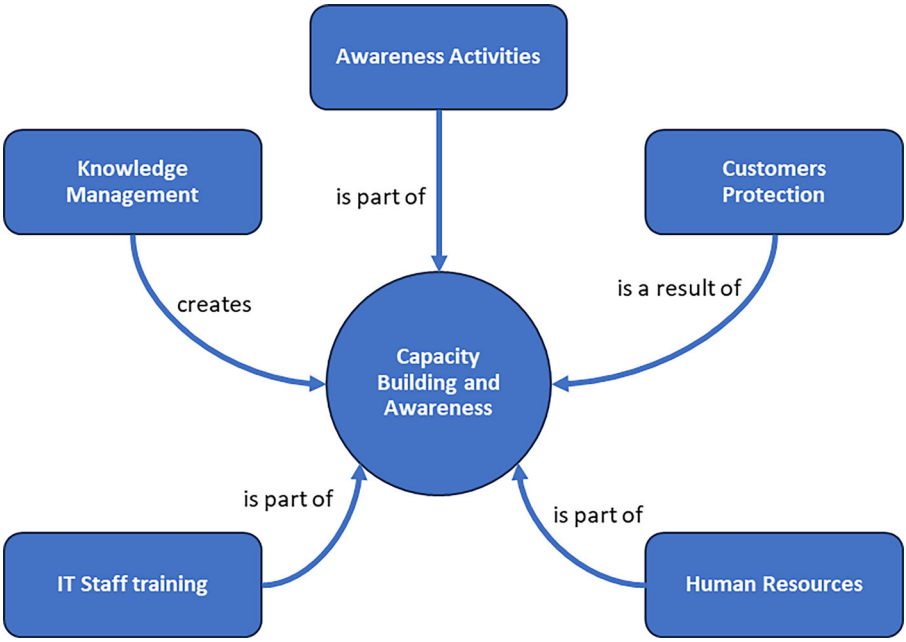

Fig. 8 The relationship of Capacity Building and Awareness and other factors

5.1.3 Forming stable groupings of items

To thoroughly understand the outcomes, a topic analysis [50] was conducted using semantic correlations [55] on the 36 items. The goal is to combine and compare the coded ideas (items). This leads to analysing and contrasting the interviews and the essential elements related to risks and cybersecurity controls that need to be implemented for FinTech firms. The analysis incorporated any extra categorisations that may have arisen from the participants' opinions. Several of them generated a distinct theme and established valid categories of objects.

5.1.4 Creating patterns

Pattern creation is grouping 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 [56]. Defining the most relevant patterns may assist in establishing fundamental principles of a cybersecurity framework for FinTech. For example, the relationships between several emerging themes related to the people factor are shown in Fig. 8. It shows that cybersecurity awareness activities are part of *Capacity Building and Awareness's* main theme. All respondents mentioned the significance of staff awareness training and its frequency in leveraging cybersecurity awareness and capacity building.

While discussing cybersecurity *Regulation and Governance*, most respondents emphasised the importance of following the Central Bank of Bahrain (CBB) Rule

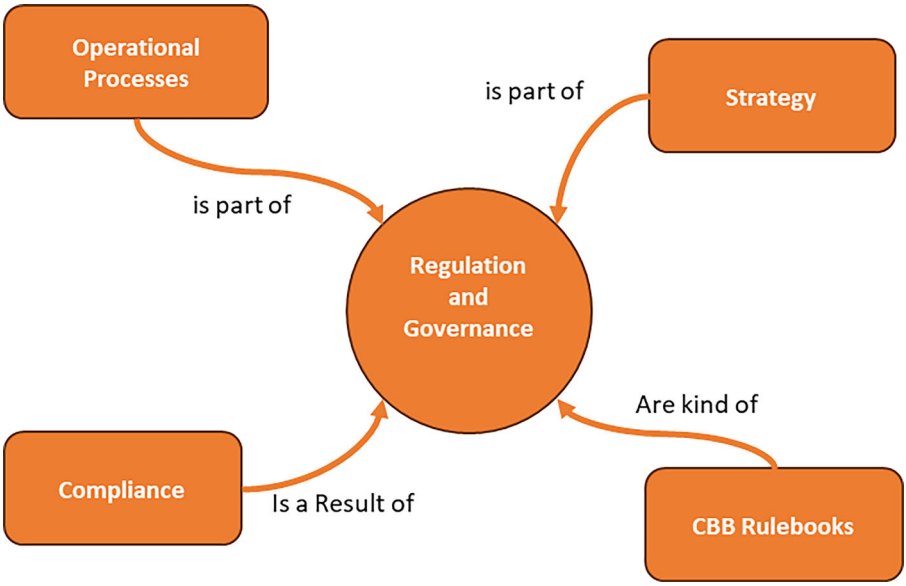

Fig. 9 The relationship of Regulation and governance and other factors

Books as they contain mandated guidelines and control from the primary financial regulator in Bahrain (Fig. 9). FinTech must go through the sandbox check to validate their compliance with all rules and regulations.

Twelve participants considered the risk management concept to include areas such as asset protection, data protection, and vulnerability assessment (Fig. 10).

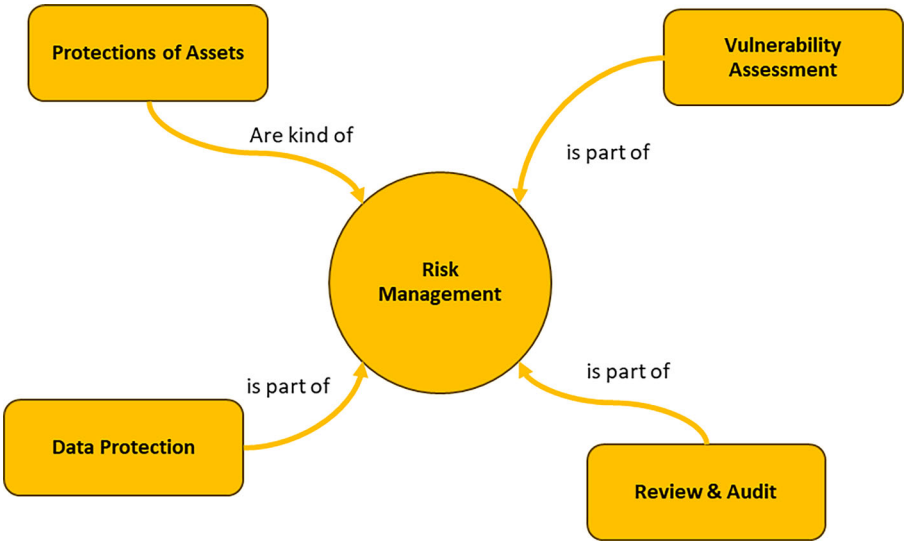

Fig. 10 The relationship between Risk Management and other factors

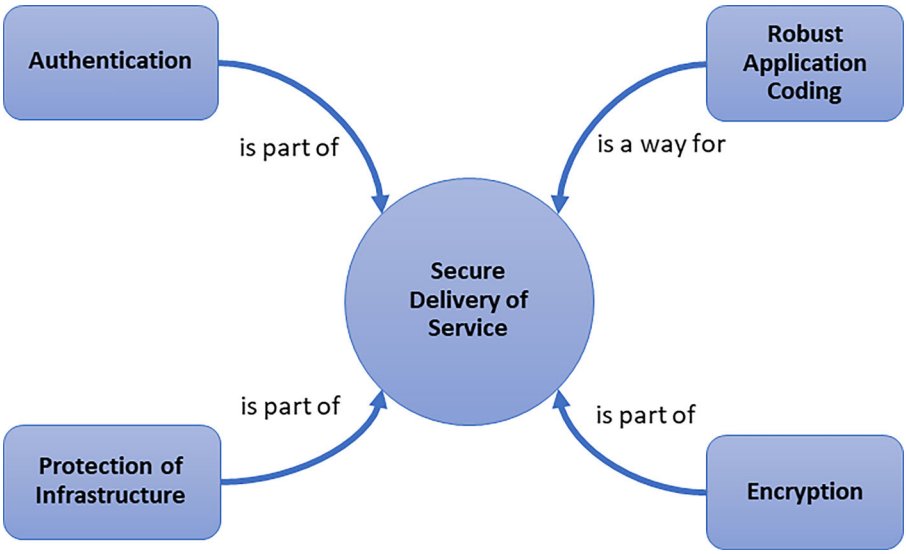

Fig. 11 The relationship between Secure Delivery of Service and other factors

Figure 11 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. They point out that users should be forced to verify themselves using a tool when initiating a transaction or accessing confidential data. Multi-factor authentication (MFA), including biometrics, should be considered.

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 cyber-

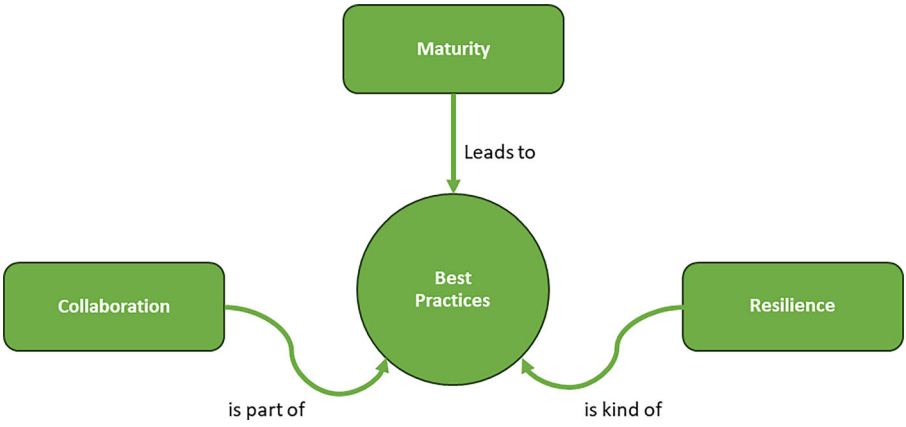

Fig. 12 The relationship between Best Practices and other factors

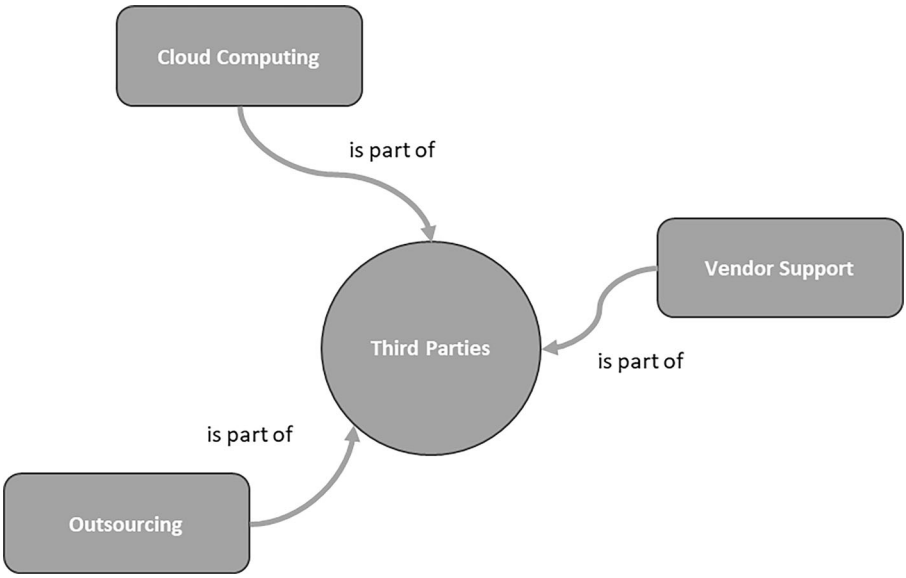

Fig. 13 The relationship of Third Parties and other factors

security of their systems, the FinTech IT department should implement and execute worldwide *Best Practices* cybersecurity systems (Fig. 12). They should be able to detect and respond to new cybersecurity threats as they arise.

Furthermore, as the discussion about third parties (Fig. 13) goes deeper, there is an issue regarding outsourcing financial organisations and potential threats to financial data security. It's important to mention that when organisations outsource specific software and services built by third parties, this could lead organisations to experience financial data breaches and other adverse events. We understand that it potentially threatens organisations' financial information as they would have access to privileged systems.

5.1.5 Building structures

This stage entails putting together collections of all created 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. The relationships between the patterns are shown in Fig. 14 using a produced conceptual map from Nvivo.

To generate a comprehensive view of the cybersecurity controls for FinTech institutes, groupings of patterns discovered in the previous step were combined to create the proposed framework. As a result, the most significant revision of the risks and cybersecurity controls was grouping the 36 items into six principles. The total weight of each factor was estimated by the weight focus given by respondents throughout interview talks in terms of word count.

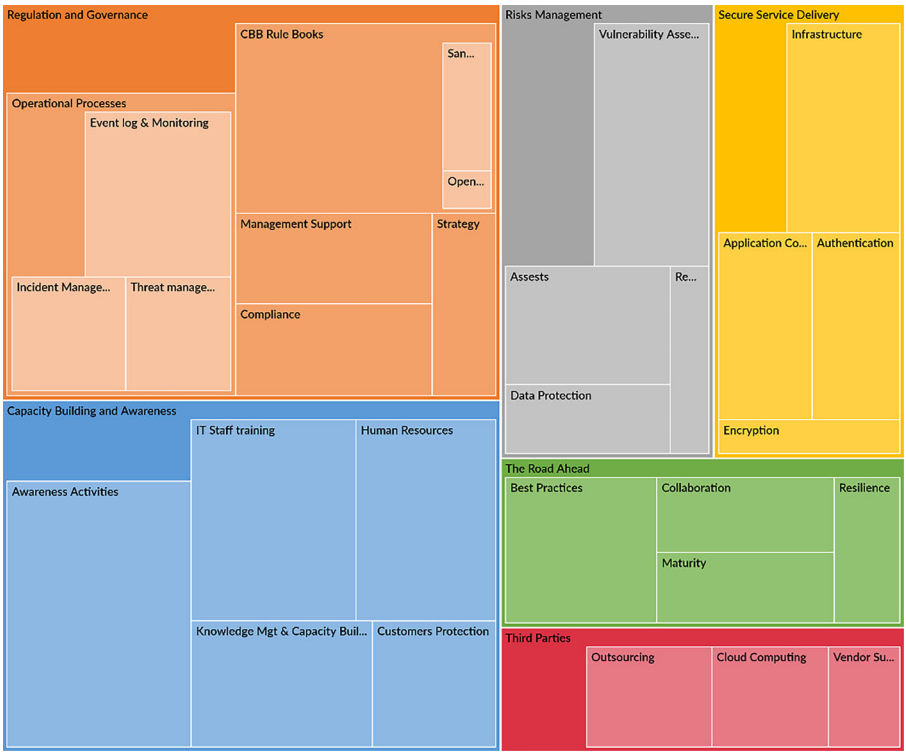

Fig. 14 The Relationships between the Patterns and the Conceptual Map

The empirical findings helped us refine the developed framework to make it more applicable to the FinTech environment while also supporting them. Respondents focused more on FinTech's considerable Regulation and Governance, Capacity Building and Awareness for security measures.

Six themes and 36 supporting patterns were obtained from the analysis of the collected data of the sample groups. Table 5 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.

Figure 15 depicts the percentage coverage of the resulting theme and fundamental cybersecurity principles as referenced by the participants. 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. Indeed, the most effective level of knowledge and skill necessary is managing risks, compliance, and security.

Table 5 Resulting themes

Themes/Principles	Codes	Ref	%
Regulation and Governance	11	173	29.22297
Capacity Building and Awareness	6	154	26.01351
Risk Management	5	85	14.35811
Secure Service Delivery	5	76	12.83784
Best Practices	5	60	10.13514
Third Parties	4	44	7.432432
	36	*592*	*100*

5.2 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 innovations in Bahrain, including regulatory and supervisory authorities, improve their supervisory frameworks, policy measures, and cooperation on FinTech services, focusing 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 6.

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 Figs. 14, 15 and 16. In Fig. 14 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 Fig. 15, 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. Finally, Fig. 16 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, Fig. 16 includes a list of

Table 6 The principles affecting Bahrain's financial stakeholders

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

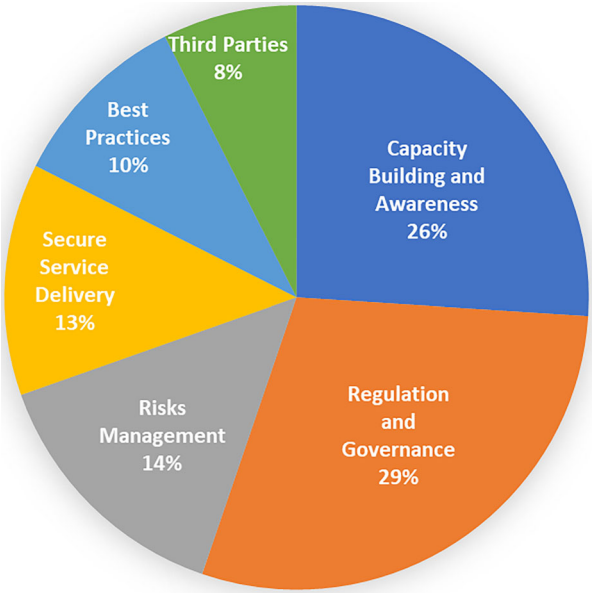

Fig. 15 The Percentage Coverage of the Resulting Themes

recommended controls, which offer further guidance and direction for effective cybersecurity implementation within each principle. Together, these figures 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.

6 Framework validation

Since this research is exploratory, the validation exercise of the proposed framework is essential as it ensures that the cybersecurity framework is aligned with financial industry best practices. The Delphi approach has been utilised for conceptual model validation and evaluation. The Delphi approach is appropriate for research involving a new or emerging trend. Researchers have extensively employed it in policy creation and judgement [57]. 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. Delphi studies may be combined with quantitative data gathering and using quantitative techniques to analyse data to provide more precise and realistic results. Triangulation is one of the approaches that may promote the validity of qualitative findings and is one of the methods employed in this study [58].

6.1 Delphi session—NGN Majlis

A Delphi session was arranged at NGN Majlis International [59] for a group of FinTech and cybersecurity experts in Bahrain's financial sector. NGN Majlis is

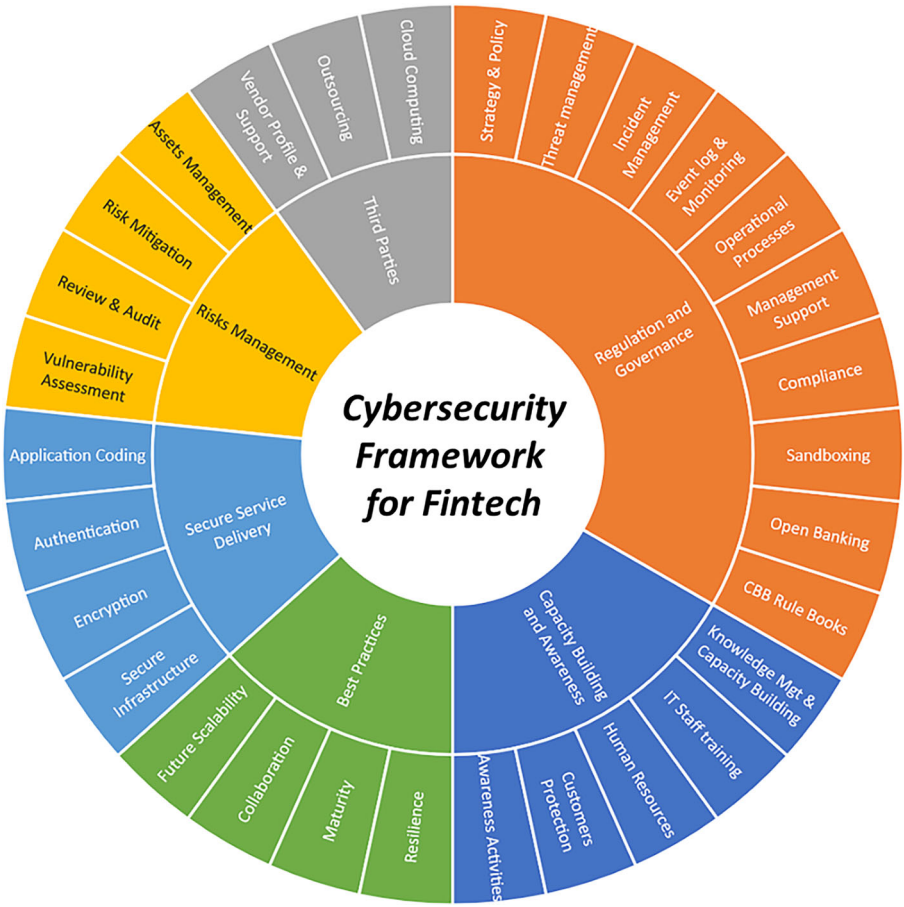

Fig. 16 The proposed cybersecurity framework for Bahrain's FinTech entities

a monthly panel discussion platform for Bahrain's ICT experts in different cybersecurity themes. In total, 42 experts attended the NGN Majlis, and 25 participated in the Delphi session. Rounds of discussions were conducted to comprehensively evaluate the framework by discussing the participants' opinions on the framework, identifying any gaps, and considering areas for improvement.

6.2 Delphi rounds

In the first round of the Delphi session, experts were surveyed systematically and asked to rate each framework's principles on a Likert scale while providing their thoughts on the framework structure and controls.

In the second round, the experts were given a new questionnaire to complete. They were asked to rank the framework's principles in order of priority while seeing the ranking from the first round, which was derived from the average points provided to each principle. The highest priority was given to the value of 1, and the lowest

Table 7 Ranking and prioritising of framework's principles as a result of Delphi session rounds

Principles	Delphi Round 1			Delphi Round 2		
	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	5.08	0.954	5
Third Parties	4.881	1.130	6	5.20	1.000	6

priority to the value of 6. Table 7 displays the ranking scores and outcomes of the framework's principles' prioritisation for both Delphi rounds.

6.3 Statistical analysis

The optimal number of Delphi session rounds remains unclear, and it should be emphasised that increasing the number of rounds may decrease response rates [60]. 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 [58]. A technique for analysing changes across Delphi rounds is provided by more complex tools, such as Kendall's W, used in this research [60]. 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 [61].

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:

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

According to Schmidt [61], 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 8.

The calculated degree of consensus (W) values from Table 6 are shown in the second column of Table 9. For each set of controls (Principles), the W values 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 ranking, according to the interpretation of Kendall's W coefficient [61].

Figure 17 demonstrates the degree of consensus based on the W values listed in Table 9.

Table 8 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

Table 9 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

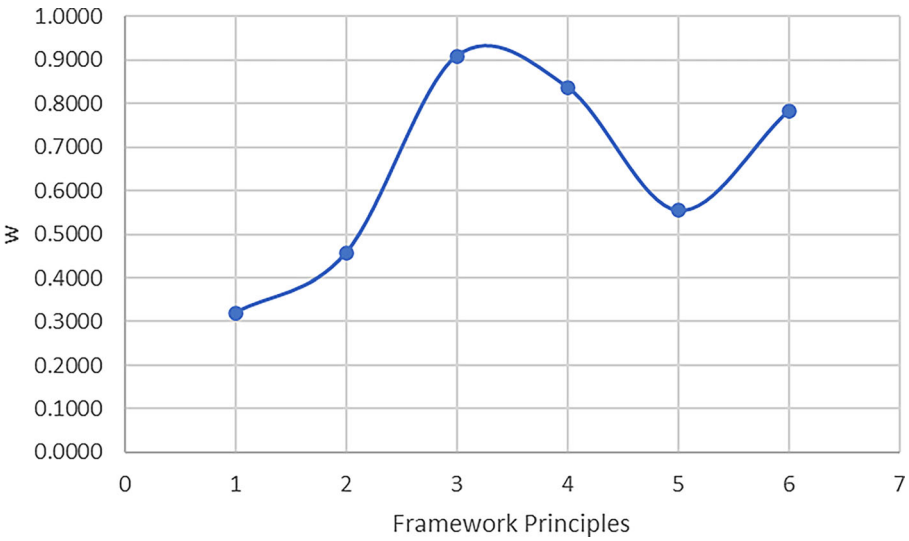

Fig. 17 The degree of consensus (W) values

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 for refining the framework according to their suggestions and comments.

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 highlighted the definition and ranking of the framework's principles and controls according to their significance in the FinTech innovations context, making them more validated and highly accepted.

7 Conclusion

The cybersecurity framework for the FinTech sector in Bahrain aims to assist these firms in establishing appropriate cybersecurity governance and robust infrastructure, as well as essential analytical and preventative measures. Moreover, the framework can aid in identifying relevant controls and guide in assessing maturity levels. The framework's adoption and implementation are critical in securing Bahrain's FinTech institutes and addressing cybersecurity threats. This ensures that cybersecurity risks are effectively addressed and well managed. The ultimate goal is to establish a trusted digital environment for both customers and FinTech companies in Bahrain.

The proposed framework encompasses various elements to address the sector's specific needs. 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 twenty-four control activities, adopting a risk-based methodology to address current and future technological advancements and potential threats.

To ensure the framework's effectiveness and applicability, 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 implementation of the framework is expected 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 contributes to the sustainable growth of the FinTech industry, boosting investor confidence and economic development 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 contributes to the establishment of an ideal, secure, and streamlined environment for FinTech innovations in Bahrain. Furthermore, adopting such a framework facilitates Bahrain's commitment to embracing technology-driven changes while prioritising security. This commitment strengthens 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 stake-

holders. This can attract both local and international businesses to establish their operations in Bahrain, positioning the country as a regional FinTech hub.

Conflict of interest S. AlBenJasim, H. Takruri, R. Al-Zaidi and T. Dargahi declare that they have no competing interests.

References

1. BFB, Bahrain Fintech Ecosystem Report 2022. Bahrain FinTech Bay, 2022.
2. Fadhul S, Hamdan A (2020) The role of "Fintech" on banking performance. In: Academic conferences international limited: reading, pp 911–914,XVII
3. Cassidy McCants JB (2023) 2023 identity theft statistics
4. Petrosyan A (2023) Global number of cyber attacks in financial sector 2013–2022. https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/#statisticContainer
5. IBM_Security (2023) Cost of a data breach report 2023
6. Barahona D (2022) Cybersecurity in fintech: top 8 fintech cybersecurity risks and challenges.
7. Bassett G et al (2021) Data breach investigations report. Verizon DBIR team. Tech Rep
8. AlBenJasim S et al (2023) Fintech cybersecurity challenges and regulations: Bahrain case study. J Comput Inf Syst p:1–17
9. Times K (2020) Over 50m cyber attacks recorded in GCC. Khaleej Times
10. (2023) GCC Cyber security market overview. In: 3rd Cyber security for energy & utilities conference
11. Davis K, Maddock R, Foo M (2017) Catching up with Indonesia's fintech industry. Law Financial Mark Rev 11(1):33–40
12. Syafrizal M, Selamat SR, Zakaria NA (2020) Analysis of cybersecurity standard and framework components. Int J Commun Networks Inf Secur 12(3):417–432
13. Didenko A (2020) Cybersecurity regulation in Singapore's financial sector: protecting fintech 'ants' in a jungle full of 'elephants. UNSW Law Research
14. Suryono RR, Budi I, Purwandari B (2020) Challenges and trends of financial technology (fintech): a systematic literature review. Information 11(12):590
15. Eickhoff M, Muntermann J, Weinrich T (2017) What do fintechs actually do? A taxonomy of fintech business models
16. Basole RC, Patel SS (2018) Transformation through unbundling: visualizing the global fintech ecosystem. Serv Sci 10(4):379–396
17. Hung JL, Luo B (2016) Fintech in Taiwan: a case study of a bank's strategic planning for an investment in a fintech company. Financial Innov 2(1)
18. Gomber P, Koch J-A, Siering M (2017) Digital finance and fintech: current research and future research directions. J Bus Econ 87(5):537–580
19. Al-Shakar A (2017) Entrepreneurship: a new era for Bahrain's economy? Glob Policy 8(3):413–416
20. Haddad C, Hornuf L (2019) The emergence of the global fintech market: economic and technological determinants. Small Bus Econ 53(1):81–105
21. Abdelghani E et al (2021) Islamic banks financing of fintech start-ups in Oman: an exploratory study. J Muamalat Islam Finance Res 18(1):55–65
22. Mehrotra A (2019) Financial inclusion through fintech—a case of lost focus. In: 2019 international conference on automation, computational and technology management (ICACTM). IEEE,
23. Stewart H, Jürjens J (2018) Data security and consumer trust in fintech innovation in Germany. Inf Comput Secur 26(1):109–128

24. Addae JH et al (2019) Exploring user behavioral data for adaptive cybersecurity. User Model User-Adap Inter 29:701–750
25. Mian TS, Alatawi EM (2023) Exploring factors to improve intentions to adopt cybersecurity: a study of saudi banking sector. Humanit Nat Sci J
26. Ambore S et al (2017) A resilient cybersecurity framework for mobile financial services (MFS). J Cyber Secur Technol 1(3-4):202–224
27. Albasheer MO, Bashier EB (2013) Enhanced model for PKI certificate validation in the mobile banking. In: 2013 international conference on computing, electrical and electronic engineering (ICCEEE). IEEE,
28. Ahamad SS, Sastry V, Nair M (2013) A biometric based secure mobile payment framework. In: 2013 4th international conference on computer and communication technology (ICCCT). IEEE,
29. Wang J, Gupta M, Rao HR (2015) Insider threats in a financial institution. MISQ 39(1):91–112
30. Mawgoud AA et al (2019) Cyber security risks in MENA region: threats, challenges and countermeasures. In: International conference on advanced intelligent systems and Informatics. Springer,
31. Al-Ahmad W, Mohammad B (2012) Can a single security framework address information security risks adequately. Int J Digit Inf Wirel Commun 2(3):222–230
32. Kaur G et al (2021) Cybersecurity policy and strategy management in fintech. In: Understanding cybersecurity management in fintech: challenges, strategies, and trends, pp 153–166
33. Barlette Y, Fomin VV (2010) The adoption of information security management standards: a literature review. In: Information resources management: concepts, methodologies, tools and applications, pp 69–90
34. Schlarman S (2007) Selecting an IT control framework. EDPAC 35(2):11–17
35. Sipior JC, Ward BT (2008) A framework for information security management based on guiding standards: a United States perspective. Issues Informing Sci Inf Technol 5:51–60
36. Knewtson HS, Rosenbaum ZA (2020) Toward understanding FinTech and its industry. Manag Finance
37. Schilirò D (2021) Fintech in Dubai: development and ecosystem. IBR 14(11):1–61
38. Turcan RV, Deák B (2021) Fintech–stick or carrot–in innovating and transforming a financial ecosystem: toward a typology of comfort zoning. Foresight
39. Kaur G, Habibi Lashkari Z, Habibi Lashkari A (2021) Cybersecurity policy and strategy management in fintech. In: Understanding cybersecurity management in fintech. Springer, pp 153–166
40. Brotby K (2009) Information security governance: a practical development and implementation approach vol 53. John Wiley & Sons
41. Brock J et al (1999) Information security risk assessment practices of leading organizations. Director, USGAO. http://www.gao. gov/special. pubs/ai00033. pdf. Accessed 20 Mar 2009
42. Keenan M (2015) Research methods. Salem Press Encyclopedia
43. Saunders M, Lewis P, Thornhill A (2016) Research methods for business students, 7th edn. Pearson Education, Nueva York
44. Knox K (2003) A researcher's dilemma—philosophical and methodological pluralism. Electron J Bus Res Methods 2(2):145–154
45. Venable JR (2011) Incorporating design science research and critical research into an introductory business research methods course. Electron J Bus Res Methods 9(2):119–129
46. Silverman D (1998) Qualitative research: meanings or practices? Info Systems J 8(1):3–20
47. Suri H (2011) Purposeful sampling in qualitative research synthesis. Qual Res J 11(2):63–75
48. Williams C (2007) Research methods. J Bus Econ Res 5(3)
49. Sachdeva JK (2019) Business research methodology. Himalaya Publishing House, Chennai
50. Leech NL, Onwuegbuzie AJ (2011) Beyond constant comparison qualitative data analysis: Using NVivo. Sch Psychol Q 26(1):70
51. Clarke V, Braun Commentary V (2017) Thematic analysis. J Posit Psychol 12(3):297–298
52. Leech NL, Onwuegbuzie AJ (2007) An array of qualitative data analysis tools: a call for data analysis triangulation. Sch Psychol Q 22(4):557
53. LeCompte MD (2000) Analyzing qualitative data. Theory Pract 39(3):146–154
54. Tellis W (1997) Introduction to case study. TQR 3(2):1–14
55. Spradley JP (1979) The ethnographic interview. Waveland Press
56. Claes J et al (2015) The structured process modeling theory (SPMT) a cognitive view on why and how modelers benefit from structuring the process of process modeling. Inf Syst Front 17(6):1401–1425
57. Linstone HA, Turoff M (1975) The delphi method. Addison-Wesley Reading, MA
58. Babazadeh Y et al (2022) Identifying key indicators for developing the use of blockchain technology in financial systems. Int J Res Ind Eng 11(3):246–257
59. International N (2022) About NGN. https://www.ngnintl.com/about-us/

60. Beiderbeck D et al (2021) Preparing, conducting, and analyzing Delphi surveys: cross-disciplinary practices, new directions, and advancements. MethodsX 8:101401
61. Schmidt RC (1997) Managing Delphi surveys using nonparametric statistical techniques. Decis Sci 28(3):763–774