


**Please cite the Published Version**

AlBenJasim, Salah, Dargahi, Tooska , Takruri, Haifa and Al-Zaidi, Rabab (2024) Fintech cybersecurity challenges and regulations: Bahrain case study. Journal of Computer Information Systems, 64 (6). pp. 835-851. ISSN 0022-0310

**DOI:** <https://doi.org/10.1080/08874417.2023.2251455>

**Publisher:** Taylor & Francis

**Version:** Published Version

**Downloaded from:** <https://e-space.mmu.ac.uk/633047/>

**Usage rights:**  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

**Additional Information:** This is an open access article which originally appeared in Journal of Computer Information Systems, published by Taylor and Francis

**Enquiries:**

If you have questions about this document, contact [openresearch@mmu.ac.uk](mailto:openresearch@mmu.ac.uk). Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

## FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study

Salah AlBenJasim, Tooska Dargahi, Haifa Takruri & Rabab Al-Zaidi

**To cite this article:** 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)

**To link to this article:** <https://doi.org/10.1080/08874417.2023.2251455>



© 2023 The Author(s). Published with  
license by Taylor & Francis Group, LLC.



Published online: 01 Sep 2023.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

# FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study

Salah AlBenJasim<sup>a</sup>, Tooska Dargahi<sup>b</sup>, Haifa Takruri<sup>a</sup>, and Rabab Al-Zaidi<sup>a</sup>

<sup>a</sup>University of Salford, Manchester, UK; <sup>b</sup>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.<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup>



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."<sup>4</sup>

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.

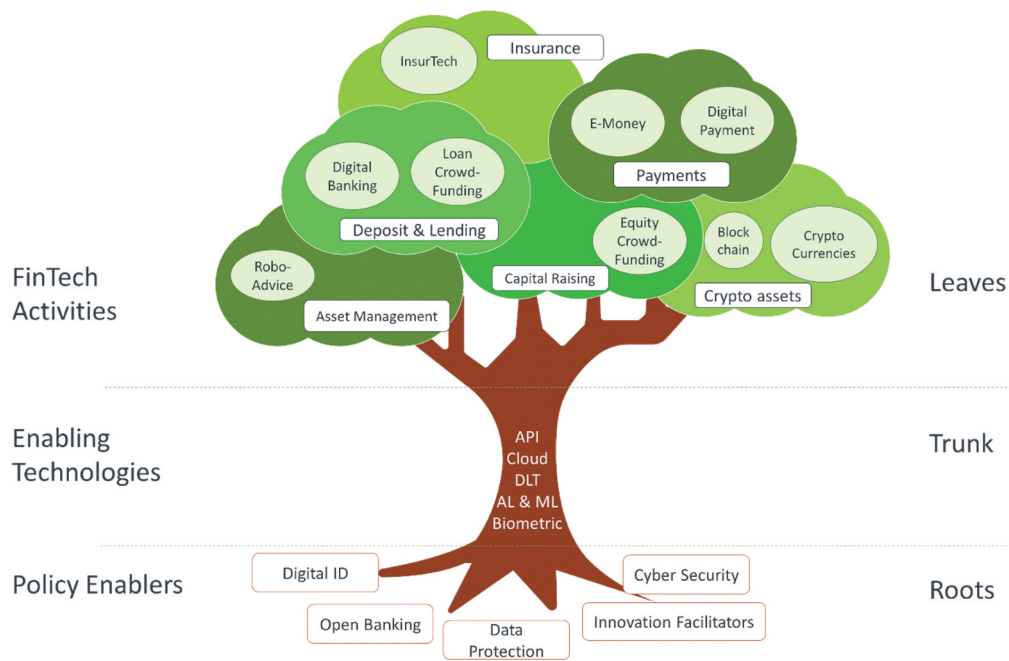
After the global financial crisis in 2008, advances in e-finance and mobile technologies for financial organizations fueled FinTech innovation. Integration in financial system innovation, Internet technology, social networking services, social media, artificial intelligence, cloud computing, and big 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.<sup>5</sup> 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,

**CONTACT** Salah AlBenJasim  S.K.Albenjasim@edu.salford.ac.uk  School of Science, Engineering & Environment, University of Salford, New SEE Building, Manchester M5 4WT, UK

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.



**Figure 1.** FinTech tree: a taxonomy of the FinTech environment.<sup>4</sup>

**Table 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)

and operations of institutes that adopt the FinTech paradigm. Table 1 demonstrates the state of a data breach in Europe, the Middle East, and Africa (EMEA), as per the Data Breach Investigations Report 2021.<sup>6</sup>

According to Trend Micro, a combined 56,873,271 e-mail, URL, malware, and banking malware attacks were recorded in the Gulf Cooperation Council (GCC) region during the first half of 2020.<sup>7</sup> 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 additional 2,294 banking malware incidences.

This paper presents a Systematic Literature Review (SLR) of FinTech cybersecurity concerns and existing risk management strategies. It helps to identify similarities across globally recognized cybersecurity standards and frameworks. Bahrain is used as a case study to

explore key characteristics and factors that were not fully addressed while adopting such standards. The results can assist Bahrain's financial regulators understand 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.

### Research goals

The purpose of this paper is to show the findings of employing a replicable technique to collect and synthesize 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 by providing answers to the following questions:

- (1) What are the cyber challenges facing FinTech companies?
- (2) What solutions exist in the literature to overcome these challenges?
- (3) Are the existing regulatory frameworks efficient and sufficient?

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.

## Prior research

There have been relatively few Systematic Literature Reviews (SLRs) done on the topic of FinTech and Cybersecurity. Zavolokina et al.<sup>8</sup> highlighted that FinTech was more than just the use of information technology in finance. FinTech may alternatively be viewed as start-ups, services, technologies, firms, digitalization, industry, new generations, opportunity, products, and risks, according to certain literature. Mehrban et al.,<sup>9</sup> provide a comprehensive survey of FinTech by reviewing the most recent and anticipated financial industry privacy and security issues. The research paper provides a comprehensive analysis of 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.<sup>10–12</sup> Furthermore, researchers have examined the different cybersecurity measures that FinTech companies might put in place to shield themselves and their clients against cyber-attacks.<sup>10–12</sup>

In the same domain, Taylor et al.,<sup>13</sup> sheds 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 to improve the vulnerability assessment of FinTech systems.<sup>14</sup> Vučinić et al, develop a FinTech 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 paper concludes by examining cyber risk in the FinTech sector as the most recent and significant concern emerging from these chaotic and unpredictable times.<sup>15</sup>

Despite the wide-range of literature on cybersecurity in FinTech, a few number of studies have identified research gaps and limitations. Some studies, for instance, have focused on certain types of cybersecurity threats or countermeasures, while others focused on only the perspectives of FinTech businesses, ignoring the perspectives of consumers and regulators.<sup>11</sup> 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.<sup>10</sup>

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 required to lead future research activity.

## Contributions and layout

This SLR supplements previous research by providing the following contributions for everyone interested in FinTech and cybersecurity to advance their work:

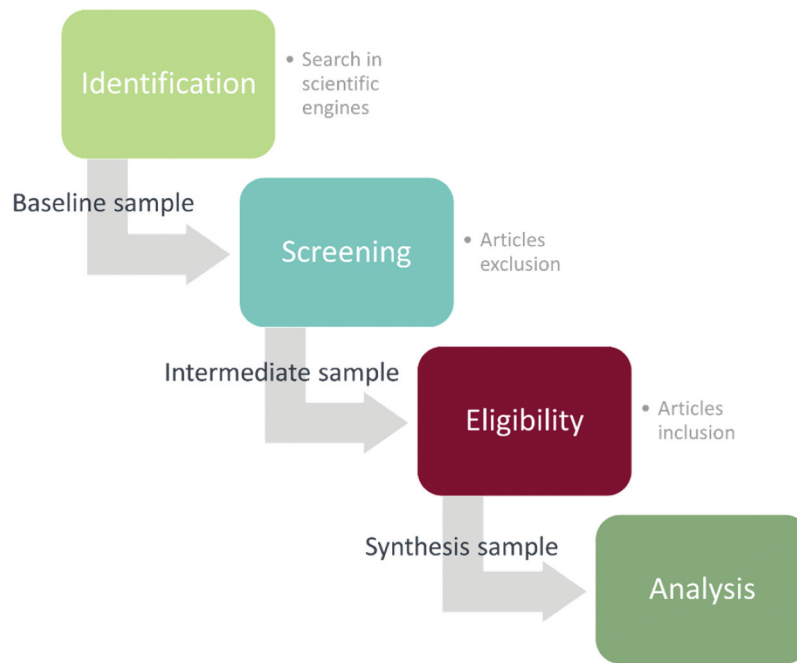
- Until November 2022, we found 153 research publications relevant to FinTech and cybersecurity. This list of publications may be used by other scholars to forward their work on the same topic.
- We present both descriptive and thematic analysis of these studies and evaluate cybersecurity challenges facing FinTechs from different perspectives, including cyber risks, system security vulnerabilities, cyber threats, cyber-attacks, and remedies to be taken.
- We provide a discussion on the existing research gaps in terms of cybersecurity regulations, guidelines, controls, and frameworks for FinTech in Bahrain, and determine challenges and patterns for future research directions.

The methodology for the SLR is presented in the next section. The sub sequent section offers the descriptive analysis of findings and presents a thematic analysis of the collected sample. Moreover, we highlight and discuss the discovered synergies across FinTech and cybersecurity frameworks, as well as relevant gaps and research opportunities. Finally, we conclude this paper with light shaded on future work.

## Methodology

Literature reviews are useful sources for knowledge generation by systematically assembling existing scientific work and using direct or meta-analysis of explicit or tacit information synthesis to address particular research questions.<sup>16</sup> This work follows Schryen et al.<sup>16</sup> published standard for the SLR, resulting in an approach that is suitable for research in a variety of sectors where there may be variations in what is considered relevant.

The SLR is a technique for selecting and analyzing scientific papers to offer evidence for the identification of published research for FinTech and cybersecurity that is complete, explicit, and reputable. The SLR’s process used in this paper is shown in [Figure 2](#) using the PRISMA set layout, which stands for Preferred Reporting Items for Systematic Reviews and Meta-Analyses.<sup>17</sup> The resulting PRISMA structure takes into account an initial batch of papers, known as the baseline sample, which was found using keywords in scientific search engines. This sample



**Figure 2.** PRISMA set layout for the systematic literature review.

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 limit down the final sample for analysis, referred to as the synthesis sample. Finally, the synthesis sample is then subjected to a descriptive analysis before being reviewed through a thematic analysis aimed at addressing the research questions.

### Search process

The search for publications was conducted using four major indexed electronic scientific databases:

- Scopus ([www.scopus.com](http://www.scopus.com))
- Web of Science ([www.webofknowledge.com](http://www.webofknowledge.com))
- Scholar ([scholar.google.com](http://scholar.google.com))
- ScienceDirect ([www.sciencedirect.com](http://www.sciencedirect.com))

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

### Searching criteria definition

The criteria for searching are based on the following keywords:

- (1) Cybersecurity
- (2) FinTech
- (3) Bahrain

Table 2 lists all search queries that were used to identify the first batch of papers:

### Papers assessment

After the search is completed, the articles undergo screening based on the criteria for inclusion/exclusion. This often entails checking if papers' titles and abstracts satisfy the requirements. A total of 153 publications centered around the subject were initially identified. Nevertheless, to ensure a current perspective, publications from the period between 2016 and 2022 were selected, with some older but important articles and references included. This has reduced the publications to 126. Further filtering 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 that are related to the topic and matches the screening criteria.

Furthermore, to assess the publications chosen; EndNote software was used to keep track of the author's comments on each of them. EndNote keeps useful

**Table 2.** Search queries.

Database	Search Queries
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"



records, such as the paper's title, authors, publication year, reference, abstract, and keywords.

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 of the publications. The following areas were specifically considered:

- (1) A review of the FinTech and cybersecurity concepts and definitions;
- (2) Description of the 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 taken into account.

### Findings and thematic analysis

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

**Table 3.** Word count.

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
Organizations	13	32	0.28
Bahrain	7	30	0.26

### Descriptive analysis of search results

The word count in terms of “% weight” (Table 3), 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 words count as shown in Figure 3. 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 text being analyzed.

### Thematic analysis

A meta-analysis is carried out to dig further into FinTech-related issues. NVIVO software is used to do selective coding, customizing it to the study question's



**Figure 3.** Word cloud.

requirements. As a manner of addressing the research objectives of this study, the thematic analysis categorizes the articles in the synthesis sample according to the characteristics of the frameworks these articles discuss and/or apply. The categorizations that are applied in this SLR are presented in Table 4:

There are a variety of viewpoints and definitions for cybersecurity and FinTech in the literature. Table 5 provides a set of FinTech definitions.

### Cybersecurity challenges and issues in FinTech

In the FinTech business, cybersecurity is the top challenge and a major legislative concern.<sup>23</sup> Cyber attacks pose a threat to 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 serious issues in the areas of privacy, cybersecurity, denial of service attacks, insider threat, malware injection, insecure APIs, shared vulnerabilities, and data security.<sup>24</sup> Table 6 lists the major challenges and issues in FinTech.

**Table 4.** Thematic analysis categorization.

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

**Table 5.** A set of FinTech definitions.

Fintech Definitions	Reference
FinTech, a mixture of financial and technology may have been around for a while. One of this term's first uses goes back to the 1980s	18
"Fintech is an industry composed of companies that use technology to make financial systems and the delivery of financial services more efficient"	19
"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."	20
"a cross-disciplinary subject that combines Finance, Technology Management and Innovation Management."	21
"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."	21
"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."	22

**Table 6.** Challenges and issues in FinTech.

Challenges and Issues in FinTech	Reference
Risks in business operations	25–30
Threats in FinTech	29,31–33
Regulatory requirements	18,24,34
Importance of experimental data	9,34
Financial privacy protection	35–38

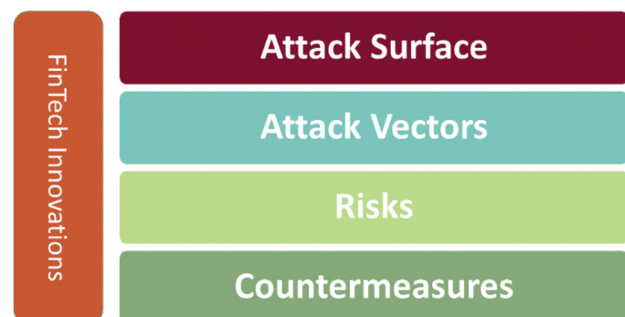
The common context that repeats in several cybersecurity definitions as provided in Table 7 were considered from some research papers:

As the financial industry as a whole continues to further embrace digitization, so does the difficulty of protecting consumer data from cyberattacks, which are facilitated by an ever-growing attack surface. Scheau et al,<sup>44</sup> 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 4, demonstrates the following levels and how they are linked to the cyber threats for FinTech businesses:

- The organizational assets that a hacker may use to access FinTech systems make up the attack surface. This surface, which comprises human, digital, and

**Table 7.** Cybersecurity definitions.

Cybersecurity Definitions	Reference
"The ability to protect or defend the use of cyberspace from cyber-attacks"	39
"Preservation of confidentiality, integrity, and availability of information in the cyberspace"	40
"All activities necessary to protect cyberspace, its users and impacted persons from cyber threats"	41
"The protection of information assets by addressing threats to information processed, stored, and transported by the internet- worked information systems"	42
"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"	43



**Figure 4.** Cyber threats for FinTech businesses.



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.

As FinTech businesses are heavily reliant on their information systems, a well-structured framework would be essential to them. By following recognized information security standard, 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.

### Cybersecurity frameworks

Cybersecurity in FinTech is a relatively new technology focus, so there is no dedicated cybersecurity framework for the field. However, there are already some general information security frameworks and standards that regulators request businesses to follow to stay safe against cyber-attack. These frameworks could be considered for FinTech infrastructure. The governance bodies and related components in each cybersecurity standard or framework are presented in [Table 8](#).

These standards and frameworks may be used as a reference, developed, modified, or integrated with other standards as required for the purpose of addressing unique issues or auditing for conformity with laws or regulations in place in a certain industry or nation.<sup>49</sup> Furthermore, an analysis is carried out to identify whether any comparable components exist across all standards and frameworks as shown in [Table 9](#).

Three to eleven similar components are owned by the selected five standards and frameworks, based on an analysis of the many parts 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 to 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, however,

very detailed and strict; it includes many elements that are distinct from the general norm.

ISO implementations are widely recognized, particularly in the financial sector, as a result of regulatory compliance requirements. Despite the fact that it is the simplest to automate and use for developing information security policies and performing automated information security risk assessments, many organizations that undertake ISO certifications concentrate on marketing benefits and neglect to recognize that being certified does not always imply that you are secure.

In the other side, because the NIST framework is very system-oriented and excludes organizational matters, there is an absence of a comprehensive view of cybersecurity risk management. NIST is primarily aimed at large organizations and may not be applicable to small businesses. In contrast to ISO 27001, NIST prescribes not only a risk assessment methodology, but also at least some of the risk assessment. NIST, like ISO27000, offers a set of security measures as well as 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, having it implemented properly would demonstrate a greater understanding of security needs and would strengthen enterprises' immunity to both external and internal threats.

A GDPR standard is often an obligation that the responsible organization, 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 organizations where IT is not mission-critical or needed for existence, ISACA published a lite version of COBIT named "COBIT Quick Start" to address complexity matter. This version of COBIT is referred to as a special form of COBIT and may be used as a baseline. It may also be used by businesses as a foundation for their transition to a decent level of cybersecurity management and governance.

From [Table 9](#), some areas like incident management, security assessment, resilience, and monitoring are not being addressed well in the analyzed standards, while NIST framework offers a higher coverage of all other components.

**Table 8.** Governance bodies and frameworks.

Governance bodies and Frameworks	Description	Governance Type	Region	Components	Reference
NIST	The National Institute of Standards and Technology <sup>39</sup> is an NGO that specializes in cybersecurity which publishes a Cybersecurity framework that can be used in practically any sector.	Framework	USA	<ul style="list-style-type: none"> <li>• Asset Management</li> <li>• Business Environment</li> <li>• Governance</li> <li>• Risk Assessment</li> <li>• Risk Management Strategy</li> <li>• Access Control</li> <li>• Awareness and Training</li> <li>• Data Security</li> <li>• Information Protection Processes and Procedures</li> <li>• Protective Technology</li> <li>• Anomalies and Events</li> <li>• Security Continuous Monitoring</li> <li>• Detection Processes</li> <li>• Response Planning</li> <li>• Communications</li> <li>• Analysis</li> <li>• Mitigation</li> <li>• Improvements</li> <li>• Recovery Planning</li> </ul>	3,24,45–47
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	<ul style="list-style-type: none"> <li>• Builds and maintain a secure network,</li> <li>• Protect cardholder data,</li> <li>• Maintain a vulnerability management program,</li> <li>• Implement strong access control measures,</li> <li>• Regularly monitor and test networks,</li> <li>• Maintain an information security policy</li> </ul>	48,49
COBIT	COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for IT management and IT governance.	Framework	Global	<b>Governance of Enterprise IT</b> <ul style="list-style-type: none"> <li>• Evaluate, Direct and Monitor (EDM)</li> </ul> <b>Management of Enterprise IT</b> <ul style="list-style-type: none"> <li>• Align, Plan and Organise (APO)<sup>50</sup></li> <li>• Build, Acquire and Implement</li> <li>• Deliver, Service and Support (DSS)</li> <li>• Monitor, Evaluate and Assess (MEA)</li> </ul>	48,49,51,52
ISO 27001	The ISO 27001, known as the information security management standard,	Standard	Global	<ul style="list-style-type: none"> <li>• Information security policies.</li> <li>• Organisation of information security.</li> <li>• Human resource security.</li> <li>• Asset management.</li> <li>• Access control.</li> <li>• Cryptography.</li> <li>• Physical and environmental security.</li> <li>• Operations security.</li> <li>• Communications Security</li> <li>• System acquisition, development, and maintenance</li> <li>• Supplier relationships</li> <li>• Information security incident management</li> <li>• Information security aspects of business continuity management</li> </ul>	32,48,49,53
GDPR	A privacy framework that specifies how organizations must secure their customers' or users' personally identifiable information	Regulation/ Framework	EU	<ul style="list-style-type: none"> <li>• Compliance</li> <li>• Breach Response,</li> <li>• Data Governance,</li> <li>• Risk Assessment,</li> <li>• Compliance Management</li> </ul>	47,49,54

### **Examples of successful cybersecurity frameworks for FinTech from other countries**

Various effective cybersecurity frameworks have been put into practice across the global financial sector. Here are some examples from the United States, Europe, Asia, and the Middle East regions.

In the United States, the National Institute of Standards and Technology-NIST Cybersecurity

Framework is widely utilized across industries, including finance, offering guidance for private sector organizations to assess and enhance their ability to prevent, detect, and respond to cyber-attacks.<sup>53</sup> Bank of America, for example has aligned its information security controls and annual policy management cycle to the National Institute of Standards and Technology—NIST.<sup>55</sup> Similarly, the European Union's Directive on Security of Network and Information Systems (NIS Directive) enforces legal



measures to elevate cybersecurity levels, specifically 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.<sup>20</sup> 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.<sup>56</sup> 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.<sup>57</sup>

In the Middle East region, 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.<sup>58</sup> Likewise, 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.<sup>47</sup>

The more widespread FinTech innovations emerge, the more likely regulators will take notice to guarantee that the information systems underlying these innovations are properly protected and controlled.<sup>59–61</sup> In next section (Discussion and Analysis), we will further analyze the need to develop a cybersecurity framework for FinTech specifically for Bahrain.

### **Bahrain FinTech security considerations**

Despite the fact that Bahrain is a regional leader in the use of FinTech applications, there is a shortage of research in this field. Table 10 depicts the research papers that address topics related to FinTech in Bahrain.

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 sector-based rules and processes currently in place.<sup>23</sup> However, dealing with such difficulties on a local as well as international level would be one of the GCC's priorities in the future years.<sup>23</sup> Meanwhile, businesses and financial institutions must be aware that, given the rapid evolution of technology, one of their primary areas of intervention

**Table 10.** Primary studies on FinTech focused on Bahrain as a case study.

Topic	Reference
Bahrain FinTech	3,62–67
Banking regulations	3,62–65
FinTech Initiatives	3,62
Challenges	3,64–66
Cybersecurity for FinTech	3,47,68–72

must be the pre-assessment of potential threats, which, when combined with a risk-mitigation strategy, should help minimize 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.<sup>3</sup>

Casoria, 2018<sup>3</sup> analyses the current state of the legislation in Bahrain and the GCC, emphasizing 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.<sup>67</sup> 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 Bahrain FinTech Ecosystem report,<sup>73</sup> 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.<sup>74</sup>

According to Al-Mhiqani et al.<sup>69</sup> 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 of inadequate cybersecurity and growing cybercrime in Bahrain's financial sector are as follows:<sup>71</sup>

- Weak protection/authentication,
- Ignorance of encryption,
- Insufficient knowledge and awareness of security standards,
- Delays in updates and security patches,
- Ineffective backup plans,
- Overconfidence in traditional and old practices, and
- IT administrators being mixed with security professionals.

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 emphasize that factors such as legal, security, and, operational risks are amongst the difficulties their clients incur while engaging in FinTech transactions.<sup>64</sup> Furthermore, the study highlights the issues that need to be addressed. Factors influencing human awareness, such as knowledge, attitude, and behavior, 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 e-mail use, being aware of cyber risks, backing up essential data, and mandatory operating system and antivirus software upgrades.<sup>71</sup> Al-Bassam,<sup>71</sup> 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."

### **Central bank of Bahrain's cybersecurity controls for FinTech**

The Central Bank of Bahrain (CBB), has established the foundations of a 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.<sup>64</sup> 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 organizations' principles, notably the Basel Committee on Banking Supervision.<sup>64</sup> 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 to 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.<sup>47</sup> Moreover, Al-Bassam<sup>71</sup> stated that only 20% of organizations in Bahrain are prepared to withstand cyberattacks and security.

### **Discussion and analysis**

The significance of a cybersecurity framework for financial institutions must be recognized. A cybersecurity framework acts as a collection of rules, policies, and procedures to handle cyber risks brought on by many and highly advanced cyberthreats. A cybersecurity framework places a strong emphasis on a scalable, adaptable, and economical method to stop cyber-attacks and boost the organization's cyber resilience.<sup>49</sup>

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.<sup>58,75-77</sup>

According to (Timeline of Cyber Incidents Involving Financial Institutions)'s report,<sup>78</sup> more than 200 cyber incidents targeting financial institutions since 2007, and are becoming more frequent, sophisticated, and destructive. In 2017, the G20 warned that cyberattacks could "undermine the security and confidence and endanger financial stability." Based on the corresponding financial damage, the attack's severity is rated. It is crucial to note that these threats have been publicly disclosed. Since many cyberthreats in the financial industry are never reported in favor of reputation and revenue loss, the true figure is undoubtedly significantly high.<sup>78</sup>

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 teams or significant technical understanding. They should also be adaptable and customizable to



a 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.<sup>79</sup> 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 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. A customized 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.<sup>80</sup> A locally designed framework tends to grow and adapt over time while remaining closely aligned with FinTech business demands.

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

### **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.<sup>49</sup> As a result, the cybersecurity framework's characteristics differ for each organization, 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.<sup>49,81</sup>

### **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 organizational changes and resources, awareness initiatives, and day-to-day activities to ensure compliance with the established standard.<sup>48,81</sup>

### **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.<sup>50</sup> PCI DSS, for example, needs a higher level of technical skills than ISO 27,001 or COBIT, which places a greater emphasis on business knowledge. However, PCI DSS controls are mainly focused on credit card transaction-specific defenses 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.<sup>48</sup>

### **Generality**

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 covering the subject in general. Comprehensiveness is another factor to consider, since it reflects the extent to which the framework provides coverage.<sup>49</sup> ISO 27,001 is a generic standard for risk management in information security, in contrast to ISO 27,005, which is a security-specific standard. ISO 27,002 does not provide a thorough list of all controls that must be implemented, although NIST does.<sup>49,81,82</sup> The development of a realistic and systematic cybersecurity framework for FinTech is a future challenge.<sup>83–85</sup>

### **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.<sup>24</sup> Moreover, it is critical to emphasize that financial-sector regulators' activities must be coordinated with national cybersecurity plans and frameworks. This relationship is maintained by continual communication with relevant government entities, including but not limited to national intelligence and law enforcement authorities.<sup>86</sup>

In Bahrain, and in order to encourage effective use, 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, deployment post-testing.<sup>67</sup> However, no criteria are clearly mentioned concerning the Cybersecurity of these FinTechs, and their measures to assure customers' data protection and infrastructure security.

In order to effectively address the distinct challenges and risks inherent to Bahrain's FinTech industry, 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.

## Conclusion and future work

This paper discussed the existing cybersecurity issues in 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 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, guidelines, standards, and frameworks.
- (3) The 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.

Although a variety of approaches for addressing cybersecurity challenges in FinTech have been established,<sup>87</sup> none of them take into account the weakest link which is the human factor that might be exploited by cyberattacks. Furthermore, the papers examined do not approach cybersecurity from a sole management standpoint, but rather from an IT perspective.

Al-Ahmad, et al, interpret that standard certification does not always imply that a FinTech is secure.<sup>88</sup> If not maintained appropriately, cybersecurity certifications might create an illusion of security. Additionally, since the standards are quite system-oriented, excluding organizational 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.<sup>88</sup> 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.<sup>12</sup> To solve this issue, a light version is recommended that may be utilized 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.<sup>88</sup>

The findings of the meta-analysis indicate that the constraints of FinTech research begin with identifying the FinTech framework,<sup>83,85</sup> which includes business models and models tailored to each organization's culture. These factors have a significant impact on national regulations and policies.<sup>5,87,89,90</sup> This sector necessitates conceptual frameworks that must be adjusted to technology advancements.<sup>87</sup> As a result, numerous countries have implemented the regulatory sandbox approach (FinTech start-up incubation), as seen in Singapore and Bahrain.<sup>59,62,91,92</sup> FinTech demands a lot of personal data, therefore keeping an eye on the platform is also important for consumer data protection.<sup>93</sup> The standard of data protection and infrastructure security must be regularly improved on this basis.<sup>49</sup> 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 behavioral models.<sup>8,32,47,84,93-95</sup> Collaboration with other businesses on the FinTech business model is also conceivable.<sup>87</sup> 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.<sup>48</sup> FinTech must also be considered part of education to prepare prospective employees for the market.<sup>9</sup>

This paper uses a reproducible method to gather and synthesize 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.

In future work, we aim to illustrate the critical aspects involved in developing a cybersecurity framework for FinTech specifically for Bahrain. Through research questionnaires, and in-depth interviews of executives and business owners, we aim to propose a cybersecurity framework that will incorporate key factors that were not addressed with the current regulations or standards. Such a framework will raise the level of cybersecurity and create a trusted electronic environment for both the customers and FinTech companies in Bahrain. Following same practice with further study, this can be generalized to the Gulf Cooperation Council (GCC) region in the future.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## References

1. Eyal I. Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*. 2017;50(9):38–49. doi:10.1109/MC.2017.3571042.
2. Schueffel P. Taming the beast: a scientific definition of fintech. *J Innovation Manage*. 2016;4(4):32–54. doi:10.24840/2183-0606\_004.004\_0004.
3. Casoria M. Cybersecurity as enterprise risk within and beyond the Bahraini legal framework. *KnE Eng*. 2018;3:37–51. doi:10.18502/keg.v3i7.3071.
4. Ehrentraud J, Ocampo DG, Garzoni L, Piccolo M. FSI insights. 2020.
5. Davis K, Maddock R, Foo M. Catching up with Indonesia's fintech industry. *Law Financ Mark Rev*. 2017;11(1):33–40. doi:10.1080/17521440.2017.1336398.
6. Bassett G, Hylender CD, Langlois P, Pinto A, Widup S. Data breach investigations report. Verizon DBIR Team, Tech Rep; 2021.

7. Times K. Over 50m cyber attacks recorded in GCC. *Khaleej Times*. 2020.
8. Zavolokina L, Dolata M, Schwabe G, editors. *FinTech transformation: how IT-enabled innovations shape the financial sector*. FinanceCom. Springer; 2016. doi:10.1007/978-3-319-52764-2\_6.
9. Mehrban S, Nadeem MW, Hussain M, Ahmed MM, Hakeem O, Saqib S, Kiah, M.M., Abbas, F., Hassan, M., Khan, M.A. Towards secure FinTech: a survey, taxonomy, and open research challenges. *IEEE Access*. 2020;8:23391–406. doi:10.1109/ACCESS.2020.2970430.
10. Najaf K, Schinckus C, Yoong LC. VaR and market value of fintech companies: an analysis and evidence from global data. *Manage Financ*. 2020;47(7):915–36. doi:10.1108/MF-04-2020-0169.
11. Barbu CM, Florea DL, Dabija D-C, Barbu MCR. Customer experience in fintech. *J Theor Appl Electron Commerce Res*. 2021;16(5):1415–33. doi:10.3390/jtaer16050080.
12. Kaur G, Habibi Lashkari Z, Habibi Lashkari A, Kaur G, Habibi Lashkari Z, Habibi Lashkari A. Chapter 8- Cybersecurity policy and strategy management in FinTech. *Understanding Cybersec Manage FinTech*. 2021;153–66.
13. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-K. A systematic literature review of blockchain cyber security. *Digital Comm Netw*. 2020;6(2):147–56. doi:10.1016/j.dcan.2019.01.005.
14. McKinnel DR, Dargahi T, Dehghantanha A, Choo K-K. A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Comput Electr Eng*. 2019;75:175–88. doi:10.1016/j.compeleceng.2019.02.022.
15. Vučinić M, Luburić R. Fintech, risk-based thinking and cyber risk. *J Cent Banking Theory Pract*. 2022;11(2):27–53. doi:10.2478/jcbtp-2022-0012.
16. Schryen G, Wagner G, Benlian A. Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of is literature. 2015.
17. Moher D, Liberati A, Tetzlaff J, Altman DG. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Int J Surg*. 2010;8(5):336–41. doi:10.1016/j.ijsu.2010.02.007.
18. Group WB. Financial sector's cybersecurity: regulations and supervision. Washington DC (USA): World Bank Group; 2018.
19. Ancrì C. Fintech innovation: an overview. Presentation, board of governors of the federal reserve system; 2016 Oct 19; Washington, DC.
20. (ECB) ECB. Guide to assessments of fintech credit institution licence applications. European Central Bank. Banking Supervision; 2017.
21. Leong K, Sung A. FinTech (Financial technology): what is it and how to use technologies to create business value in fintech way? *Int J Innovation Manage Technol*. 2018;9(2):74–78. doi:10.18178/ijimt.2018.9.2.791.
22. Gray A, Leibrock M. Fintech and financial stability: exploring how technological innovations could impact the safety and security of global markets. DTCC Papers. 2017 Oct.
23. Hakmeh J. Cybercrime legislation in the GCC countries. International Security Department, Chatham

- House (The Royal Institute of International Affairs); 2018.
24. Magnuson W. Regulating fintech. *Vanderbilt Law Rev.* 2018;71:1167–226.
  25. Gai K, Qiu M, Elnagdy SA, editors. 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) New York (USA). IEEE; 2016.
  26. Liao C, Liu C-C, Chen K. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: an integrated model. *Electron Commer Res Appl.* 2011;10(6):702–15. doi:10.1016/j.elerap.2011.07.003.
  27. Nussbaumer P, Matter I, Schwabe G. “Enforced” vs. “Casual” transparency – Findings from IT-Supported financial advisory encounters. *ACM Trans Manage Inf Syst.* 2012;3(2):1–19. doi:10.1145/2229156.2229161.
  28. Shim Y, Shin DH. Analyzing China’s fintech industry from the perspective of actor-network theory. *Telecomm Policy.* 2016;40(2–3):168–81. doi:10.1016/j.telpol.2015.11.005.
  29. Gai K. A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. *Int J Comput Appl.* 2014;95(3):40–44. doi:10.5120/16578-6268.
  30. Ni J, Yu Y, Mu Y, Xia Q. On the security of an efficient dynamic auditing protocol in cloud storage. *IEEE Trans Parallel Distrib Syst.* 2013;25(10):2760–61. doi:10.1109/TPDS.2013.199.
  31. Gai K, Qiu M, Sun X, Zhao H, editor. Security and privacy issues: a survey on FinTech. International conference on smart computing and communication Shenzhen (China). Springer; 2016.
  32. Wang J, Gupta M, Rao HR. Insider threats in a financial institution. *MIS Q.* 2015;39(1):91–112. doi:10.25300/MISQ/2015/39.1.05.
  33. Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. *J Manage Inf Syst.* 2011;28(2):203–36. doi:10.2753/MIS0742-1222280208.
  34. Overy A. The challenge faced by all those in the fintech market is how to capture innovation while preserving the stability of the banking network. [www.wallenovery.com](http://www.wallenovery.com); 2018.
  35. Sánchez R, Almenares F, Arias P, Díaz-Sánchez D, Marín A. Enhancing privacy and dynamic federation in IdM for consumer cloud computing. *IEEE Trans Consum Electron.* 2012;58(1):95–103. doi:10.1109/TCE.2012.6170060.
  36. Li Y, Dai W, Ming Z, Qiu M. Privacy protection for preventing data over-collection in smart city. *IEEE Trans Comput.* 2015;65(5):1339–50. doi:10.1109/TC.2015.2470247.
  37. Li Z, Li W, Wen Q, Chen J, Yin W, Liang K. An efficient blind filter: location privacy protection and the access control in FinTech. *Future Gen Compt Syst.* 2019;100:797–810. doi:10.1016/j.future.2019.04.026.
  38. Elnagdy SA, Qiu M, Gai K, editors. 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) Beijing (China). IEEE; 2016.
  39. NISTKissel R. Glossary of key information security terms. Pennsylvania (USA): Diane Publishing; 2011.
  40. Standardization IO. Information technology; Security techniques; IT network security. Geneva (Switzerland): International Organization for Standardization; 2005.
  41. ENISA. ENISA overview of cybersecurity and related terminology. 2017.
  42. ISACA. Cybersecurity fundamentals glossary. 2016.
  43. CNSSI. Committee on national security systems (CNSS) glossary. 2015.
  44. Şcheau MC, Rangu CM, Popescu FV, Leu DM. Key pillars for FinTech and cybersecurity. *Acta Universitatis Danubius OEconomica.* 2022;18(1):194–210.
  45. Huang RH. Online P2P lending and regulatory responses in China: opportunities and challenges. *European Bus Organ Law Rev.* 2018;19(1):63–92. doi:10.1007/s40804-018-0100-z.
  46. Hu Z, Ding S, Li S, Chen L, Yang S. Adoption intention of fintech services for bank users: an empirical examination with an extended technology acceptance model. *Symmetry.* 2019;11(3):340. doi:10.3390/sym11030340.
  47. Albastaki Y, Manta O. Innovative strategies for implementing FinTech in banking book. 2020. doi:10.4018/978-1-7998-3257-7.
  48. Smith W. A comprehensive cybersecurity defense framework for large organizations. Florida (USA): Nova Southeastern University; 2019.
  49. Syafrizal M, Selamat SR, Zakaria NA. Analysis of cybersecurity standard and framework components. *Int J Commun Netw Inf Secur.* 2020;12(3):417–32. doi:10.17762/ijcnis.v12i3.4817.
  50. Al Duhaidahawi HMK, Zhang J, Abdulreza MS, Sebai M, Harjan SA. Analysing the effects of FinTech variables on cybersecurity: evidence from Iraqi banks. *Int J Res Bus Social Sci.* 2020;9(6):123–33. doi:10.20525/ijrbs.v9i6.914.
  51. Kabanda G. A cybersecurity culture framework and its impact on Zimbabwean organizations. *Asian J Manage Eng Comput Sci.* 2018;3(4):17–34. doi:10.13005/ojcs14.010203.03.
  52. Malatji M, Von Solms S, Marnewick A. Socio-technical systems cybersecurity framework. *Inf Comput Secur.* 2019;27:233–72. doi:10.1108/ICS-03-2018-0031.
  53. Shen L. The NIST cybersecurity framework: overview and potential impacts. *Scitech Lawyer.* 2014;10:16.
  54. Canelón J, Huerta E, Incera J, Ryan T. A cybersecurity control framework for blockchain ecosystems. *Int J Digital Account Res.* 2019;19:103–44. doi:10.4192/1577-8517-v19\_5.
  55. Bnak of America. Risk management and cyber security framework. USA: Global Institutional Consulting; 2019.
  56. Didenko AN. Cybersecurity regulation in singapore’s financial sector: protecting FinTech ‘Ants’ in a jungle full of ‘Elephants’. *UNSW Law Res Pap.* 2020;(20–45). doi:10.2139/ssrn.3679678.



57. Nomakuchi T, editor. A case study on fintech in Japan based on keystone strategy. 2018 portland international conference on management of engineering and technology (PICMET) Honolulu (USA). IEEE; 2018.
58. Schilirò D. Fintech in Dubai: development and ecosystem. *Int Bus Res*. 2021;14(11):1–61. doi:10.5539/ibr.v14n11p61.
59. Haddad C, Hornuf L. The emergence of the global fintech market: economic and technological determinants. *Small Bus Econ*. 2019;53(1):81–105. doi:10.1007/s11187-018-9991-x.
60. Mawgoud AA, Taha MHN, Khalifa NEM, Loey M, editors. Cyber security risks in MENA region: threats, challenges and countermeasures. International conference on advanced intelligent systems and informatics Cairo (Egypt). Springer; 2019.
61. Mulligan SP, Freeman WC, Linebaugh CD. Data protection law: an overview. *Congressional Res Serv*. 2019;45631:25.
62. Al-Shakar A. Entrepreneurship: a new era for Bahrain's economy? *Glob Policy*. 2017;8(3):413–16. doi:10.1111/1758-5899.12483.
63. Ahmed AS, Kumar M, Moh'd Ali MA, editors. Adoption of FinTech and future perspective: an empirical evidence from Bahrain on digital wallets. 2020 international conference on decision aid sciences and application (DASA) Sakheer (Bahrain). IEEE; 2020.
64. Razzaque A, Cummings RT, Karolak M, Hamdan A. The propensity to use FinTech: input from bankers in the Kingdom of Bahrain. *J Inf Knowl Manage*. 2020;19(1):2040025. doi:10.1142/S0219649220400250.
65. Abdulkarim AM. Bank users motivation for adoption of fintech services: empirical evidence with TAM in Kingdom of Bahrain. *iKSP J Innovative Writings*. 2021;1(2):1–11.
66. Raza Rabbani M, Bashar A, Khan S. Agility and fintech is the future of Islamic finance: a study from Islamic banks in Bahrain. Available at SSRN 3783171. 2021.
67. Ali H, Al Kaabi R, Ali HM, Ahmed HS, Naser M. FinTech in the Kingdom of Bahrain: an investigation of users' adoption and satisfaction. In: *InnovActive strategies for implementing FinTech in banking*. IGI Global; 2021. pp. 174–90.
68. Al-Alawi AI, Al-Bassam SA. Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf J Sci Res*. 2019;17–32. doi:10.51758/AGJSR-04-2019-0014.
69. Al-Mhiqani MN, Ahmad R, Yassin W, Hassan A, Abidin ZZ, Ali NS, Abdulkareem, K.H. Cyber-security incidents: a review cases in cyber-physical systems. *Int J Adv Comput Sci Appl*. 2018;(1):499–508.
70. AL-ALAWI AI, AL-BASSAM MSA. The significance of cybersecurity system in helping managing risk in banking and financial sector. *J Xidian Univ*. 2020;14:1523–36.
71. Al-Alawi AI, Al-Bassam SA, Mehrotra AA. Critical cybersecurity threats: frontline issues faced by Bahraini organizations. In: *Implementing computational intelligence techniques for security systems design*. IGI Global; 2020. p. 210–29. doi:10.4018/978-1-7998-2418-3.ch011.
72. Hasan S, Ali M, Kurnia S, Thurasamy R. Evaluating the cyber security readiness of organizations and its influence on performance. *J Inf Secur Appl*. 2021;58:102726. doi:10.1016/j.jisa.2020.102726.
73. BFB. Bahrain fintech ecosystem report 2022. Bahrain FinTech Bay; 2022.
74. Al-Alawi AI, Al-Hammam AH, Al-Alawi SS, AlAlawi EI. The adoption of E-Wallets: current trends and future outlook. In: *Innovative strategies for implementing FinTech in banking*. IGI Global; 2021. p. 242–62.
75. Knewton HS, Rosenbaum ZA. Toward understanding FinTech and its industry. *Manage Financ*. 2020;46:1043–60. doi:10.1108/MF-01-2020-0024.
76. Turcan RV, Deák B. Fintech—stick or carrot—in innovating and transforming a financial ecosystem: toward a typology of comfort zoning. *Foresight*. 2021;24:126–39. doi:10.1108/FS-02-2021-0052.
77. Kaur G, Habibi Lashkari Z, Habibi Lashkari A. Cybersecurity policy and strategy management in FinTech. In: *Understanding cybersecurity management in FinTech*. Springer; 2021. p. 153–66. doi:10.1007/978-3-030-79915-1\_8.
78. Project F. Timeline of cyber incidents involving financial institutions. *Carnegie Endowment Int Peace*. 2022.
79. Brothby K. Information security governance: a practical development and implementation approach. John Wiley & Sons; 2009. doi:10.1002/9780470476017.
80. Brock J, Boltz J, Doring E, Gilmore M Information security risk assessment practices of leading organizations. Director. USGAO [online]. 1999. [accessed 2009 Mar 20]. <http://www.gao.gov/special-pubs/ai00033pdf>.
81. Schlarman S. Selecting an IT control framework. *EDPAC: the EDP audit. Control Secur Newsl*. 2007;35(2):11–17. doi:10.1080/07366980601148030.
82. Knapp KJ, Knapp KJ. Cyber security and global information assurance: threat analysis and response solutions: threat analysis and response solutions. IGI Global; 2009. doi:10.4018/978-1-60566-326-5.
83. Eickhoff M, Muntermann J, Weinrich T. What do FinTechs actually do? A taxonomy of FinTech business models; 2017.
84. Abdullah EME, Rahman AA, Rahim RA. Adoption of financial technology (Fintech) in mutual fund/unit trust investment among Malaysians: unified theory of acceptance and use of technology (UTAUT). *Int J Eng Technol*. 2018;7(2):110–18. doi:10.14419/ijet.v7i2.29.13140.
85. Basole RC, Patel SS. Transformation through unbundling: visualizing the global FinTech ecosystem. *Ser Sci*. 2018;10(4):379–96. doi:10.1287/serv.2018.0210.
86. Panetta F. Fintech and banking: today and tomorrow. Rome: Speech of the Deputy Governor of the Bank of Italy; 2018 May 12.
87. Suryono RR, Budi I, Purwandari B. Challenges and trends of financial technology (Fintech): a systematic literature review. *Information*. 2020;11(12):590. doi:10.3390/info11120590.
88. Al-Ahmad W, Mohammad B. Can a single security framework address information security risks adequately. *Int J Digital Inf Wireless Commun*. 2012;2:222–30.
89. Hung JL, Luo B. FinTech in Taiwan: a case study of a Bank's strategic planning for an investment in



- a FinTech company. *Financi Innovation*. 2016;2(1). doi:[10.1186/s40854-016-0037-6](https://doi.org/10.1186/s40854-016-0037-6).
90. Gomber P, Koch J-A, Siering M. Digital finance and FinTech: current research and future research directions. *J Bus Econ*. 2017;87(5):537–80. doi:[10.1007/s11573-017-0852-x](https://doi.org/10.1007/s11573-017-0852-x).
  91. Abdelghani E, Mohammed Mispah Said O, Abdullah Mohammed A, Welcome S. Islamic banks financing of fintech start-ups in Oman: an exploratory study. *J Muamalat Islamic Finance Res*. 2021;18(1):55–65. doi:[10.33102/jmifr.v18i1.329](https://doi.org/10.33102/jmifr.v18i1.329).
  92. Mehrotra A. editor. Financial inclusion through FinTech—A case of lost focus. 2019 international conference on automation, computational and technology management (ICACTM) London (UK). IEEE; 2019.
  93. Stewart H, Jürjens J. Data security and consumer trust in FinTech innovation in Germany. *Inf Comp Secur*. 2018;26(1):109–28. doi:[10.1108/ICS-06-2017-0039](https://doi.org/10.1108/ICS-06-2017-0039).
  94. Schierz PG, Schilke O, Wirtz BW. Understanding consumer acceptance of mobile payment services: an empirical analysis. *Electron Commer Res Appl*. 2010;9(3):209–16. doi:[10.1016/j.elerap.2009.07.005](https://doi.org/10.1016/j.elerap.2009.07.005).
  95. Wonglimpiyarat J. FinTech banking industry: a systemic approach. *Foresight*. 2017;19:590–603. doi:[10.1108/FS-07-2017-0026](https://doi.org/10.1108/FS-07-2017-0026).