GENIUS INSIGHT ECONOMICS : Journal of Digital Business, Finance, and Development Studies, Vol. 01, No. 01, 50-64,

DOI: XXXXXXXXXXXXXXX
Website Journal Gie:
https://geniusinsightindonesia.com/index.php/gie/index

Cyber Governance, Operational Resilience, and Market Confidence in Financial Institutions: A Systematic Review and Normative Analysis

Hatimah[1]
Islamic Banking Study Program, State Islamic University of Palopo, Indonesia
Jumarni[2]
Islamic Banking Study Program, State Islamic University of Palopo, Indonesia
Ahmad Syawal Senong Pakata[3]
Islamic Banking Study Program, State Islamic University of Palopo, Indonesia
Sitti Fatimah[4]
Islamic Accounting Study Program, State Islamic University of Palopo, Indonesia

Abstract
Cyber risks in financial institutions can no longer be regarded as a separate technical issue, as they have a direct impact on governance structures, accountability, the continuity of critical functions, and trust in digitally mediated markets. However, the existing literature remains fragmented across governance studies, resilience studies, and market-based studies, meaning that the institutional relationships between cyber governance, operational resilience, and market confidence have not yet been adequately synthesised. This article addresses this gap by conducting a systematic literature review combined with a normative analysis to examine how these three domains are conceptualised, linked, and evaluated within financial institutions. Using PRISMA 2020 and PRISMA-S as procedural frameworks, this review identifies and synthesises 50 peer-reviewed studies, selected through a transparent screening process and eligibility criteria. The findings suggest that cyber governance should be understood as an architecture of accountability, operational resilience as the capacity for continuity and recovery, and market confidence as a trust-based institutional outcome. This review further argues that market confidence should not be reduced to post-incident market reactions, but must be understood as an ex ante institutional condition shaped by credible governance and effective resilience, and subsequently tested when disruptions occur. Conceptually, this article develops an integrated institutional framework linking these three domains. Normatively, it argues that financial institutions should be evaluated not only on the basis of formal cyber controls or disclosure practices, but also on the basis of observable institutional preparedness to maintain critical functions and trust amidst digital disruptions.

Keywords:
Cyber Governance, Operational Resilience, Market Confidence, Financial Institutions, Institutional Accountability

1. INTRODUCTION

The financial sector now operates through a highly digitalised architecture, in which core banking services, payments, trading, custody, and services that interact directly with customers rely on data, networks, platforms, and external technology providers operating continuously, rather than on isolated institutional infrastructure (Leo, 2020; Uddin et al., 2020). This transformation has expanded the sector's productive capacity and reach, yet it has also transformed cyber risk from a peripheral security issue into a structural condition within financial intermediation, as disruptions

Corresponding author

Hatimah, Islamic Banking Study Program, State Islamic
University of Palopo, Indonesia, Indonesia Email: hatimah@uinpalopo.ac.id

Final transcript accepted 24 April 2026 by Ahmad Nouruzzaman Editor-in-Chief.

now threaten not only confidentiality but also the integrity and availability of systems critical to operations (Eisenbach et al., 2022). In a highly interconnected payments and settlements environment, cyber disruptions at key nodes can propagate through liquidity channels, time, and dependencies in ways that transcend the boundaries of the initially affected institutions (Eisenbach et al., 2022; Uddin et al., 2020). Consequently, for financial institutions, digital interdependence is inseparable from institutional vulnerability: cyber exposure is embedded within the very infrastructure where the promises to pay, store value, and transfer claims are executed (Leo, 2020).

The key issue is that cyber incidents in financial institutions cannot be adequately understood as isolated technical malfunctions. As these institutions facilitate claims and services that are sensitive to trust and critical to operational continuity, cyber disruptions have a direct impact on operational continuity, organisational credibility, stakeholder trust, and the perceived reliability of market infrastructure (Gwebu et al., 2018; Kamiya et al., 2021). Empirical studies indicate that successful cyberattacks can result in shareholder wealth losses, alter risk management behaviour, damage corporate reputation, and affect business partners and market participants beyond the organisation directly targeted by the attack (Corbet & Gurdgiev, 2019; Kamiya et al., 2021; Rosati et al., 2017). Other related research indicates that data breach events affect market activity and information asymmetry, whilst reputation and post-breach response strategies determine the extent to which firm value can be protected following an incident (Rosati et al., 2017; Gwebu et al., 2018). In this context, market confidence is not an abstract backdrop to cyber events; rather, it is one of the key institutional interests that renders cyber vulnerabilities economically and regulatorily significant (Florackis et al., 2023a; Gordon et al., 2010).

However, the relevant literature remains highly fragmented. A review of cyber risk research notes that the literature is scattered across the fields of computer science, information systems, business, accounting, finance, law, and policy, making it difficult to form a unified understanding of how cyber risk is generated, regulated, disclosed, assessed, and absorbed (Liu & Babar, 2026; Uddin et al., 2020). Within this dispersed field, one strand examines cyber resilience as a conceptual and institutional response to prevention constraints; another investigates operational resilience and its uneven disclosure across the banking sector; yet another stream focuses on board attributes, oversight, and disclosures related to cybersecurity; and another stream evaluates cyber risk through share returns, market value effects, or post-breach trading behaviour (Dupont, 2019; Florackis et al., 2023; Gordon et al., 2010; Radu & Smaili, 2022; Rosati et al., 2017; Schmitz & Leoni, 2019). Each of these research streams is valuable, yet they are often conducted within disciplinary silos that prioritise technical controls, corporate-level disclosures, event study assessments, or systemic stability modelling without adequately linking these dimensions within a single institutional framework concerning financial trust (Eisenbach et al., 2022; Liu & Babar, 2026). Consequently, the literature has yielded important insights into cyber incidents and resilience, yet leaves an underdeveloped conceptual bridge between governance arrangements within financial institutions, resilience capacities across critical operations, and the formation of trust amongst investors, counterparties, customers, and regulators (Dupont, 2019; Florackis et al., 2023; Leo, 2020).

This unresolved misalignment defines the current research gap. Existing governance studies help explain how boards of directors, supervisory structures, and disclosure practices shape an organisation's cyber risk management, but do not sufficiently explain how these governance arrangements interact with operational resilience as an institutional capability that generates trust (Harel & Carmeli, 2025; Radu & Smaili, 2022). Resilience-oriented studies, on the other hand, explain why financial institutions must be able to withstand, recover from, and adapt to cyber shocks, yet do not fully link resilience to the credibility issues faced by markets under conditions of uncertainty (Dupont, 2019; Leo, 2020). Market-based studies show that cyber risks are priced, disclosed, and transmitted, yet this is generally done without a systematic synthesis of governance and regulatory frameworks that could stabilise trust ex ante rather than merely being observed ex post (Florackis et al., 2023a; Kamiya et al., 2021; Rosati et al., 2017). Therefore, what remains insufficiently synthesised is the interaction between cyber governance, operational resilience, and market confidence in financial institutions, particularly when these questions are framed not only

descriptively but also normatively in terms of what should be prioritised, mandated, and evaluated by institutions and regulators (Harel & Carmeli, 2025; Liu & Babar, 2024).

This article aims to systematically synthesise how the literature conceptualises and links cyber governance, operational resilience, and market confidence in financial institutions, as well as to develop a normative framework for evaluating the policy and supervisory arrangements that should govern the integration of these three elements. More specifically, this article seeks to: (1) identify how these three concepts are formulated and where key conceptual fragmentation still persists; (2) examine the institutional mechanisms through which cyber governance shapes operational resilience and, in turn, influences market confidence; and (3) formulate a normative framework for assessing the regulatory and supervisory expectations required to maintain confidence, continuity, and accountability in digitally mediated financial markets.

This article makes three contributions. First, conceptually, it integrates the existing literature, which traditionally treats cyber governance, operational resilience and market confidence as separate fields, and places all three within an integrated institutional framework relating to financial confidence.

Second, this article makes an analytical contribution by identifying the mechanisms through which governance arrangements, accountability structures, resilience capacities, and dependency management interact to shape the credibility of financial institutions under cyber pressure. Thirdly, this article makes a normative contribution by developing a framework for evaluating regulatory and supervisory approaches not only in terms of compliance or incident response, but also in terms of their capacity to maintain critical functions, institutional legitimacy, and trust in digitally mediated financial markets.

2. METHODOLOGY

This study This study employs a systematic literature review with a normative analysis to examine the relationship between cyber governance, operational resilience and market confidence in financial institutions. This review is systematic in a procedural sense, meaning that the literature was identified, screened, assessed for suitability, and included based on explicit and transparent criteria, rather than being collected haphazardly or cited merely for illustrative purposes. At the same time, this study is not designed as a meta-analysis and does not aim to estimate combined effects, statistically rank causal strength, or produce quantitative generalisations. Its purpose is rather to construct a structured body of literature and analyse it through structured thematic synthesis and normative evaluation (Lim et al., 2022; Sauer & Seuring, 2023; Smith & Miller, 2025).

To support transparency in the selection and reporting of studies, this review was conducted in accordance with the PRISMA 2020 guidelines, whilst the reporting of search procedures refers to PRISMA-S. In this article, PRISMA serves as a framework for documenting how studies were identified, screened, assessed for eligibility, and included, thereby enhancing the traceability of the review process. It is not intended as a claim to meta-analytic synthesis, nor as a substitute for substantive analytical reasoning. The substantive analytical work of this article lies in the systematic construction of the corpus, the thematic synthesis of selected studies, and the normative evaluation of the adequacy of concepts and institutional arguments developed in the literature (Page et al., 2021; Rethlefsen et al., 2021).

Methodologically, this article should not be read as a narrative review supplemented with PRISMA terminology. Its design is that of a systematic review in which the literature corpus is compiled through transparent and reproducible selection procedures, and subsequently analysed through thematic synthesis and normative evaluation. This combination is necessary because the issue under investigation is not limited to describing what the literature says about cyber risk in financial institutions, but extends to assessing whether existing conceptualisations of governance, resilience, and market confidence are institutionally coherent and normatively adequate for policy and supervisory purposes. The methodological contribution of this article therefore lies not in statistical aggregation, but in the structured integration and evaluation of fragmented interdisciplinary literature.

The data sources for this study are scientific journal articles obtained from major academic databases, namely Scopus, Web of Science Core Collection, ScienceDirect, SpringerLink, Wiley Online Library, Taylor & Francis Online, and Emerald Insight, with Google Scholar used to a limited extent as an additional source to ensure no relevant journal articles were overlooked. The search strategy was formulated using core terms that directly represent the scope of the articles, including "cyber governance", "cyber risk governance", "operational resilience", "digital operational resilience", "market confidence", "trust in financial institutions", "financial institutions" AND cybersecurity, "financial stability" AND cyber risk, and "resilience" AND governance AND banking OR finance. Boolean operators, exact phrase searches, and iterative refinement were used to maintain a balance between search coverage and the conceptual relevance of the results. Such a systematic approach is necessary because the literature on cyber risk in the financial sector spans the fields of finance, governance, regulation, risk management, information systems, and cybersecurity (Lim et al., 2022; Paul et al., 2021; Sauer & Seuring, 2023).

Inclusion and exclusion criteria were established a priori to ensure the study's scope remained well-defined. Studies were included if they met four main criteria: they were peer-reviewed journal articles, written in English, published between January 2020 and March 2026 — the timeframe defined in this paper—and substantially discussed at least one meaningful relationship between financial institutions, cyber risk governance, operational resilience, digital operational resilience, trust, market confidence, institutional credibility, or financial stability. Conversely, studies were excluded if they were news articles, consultancy reports, popular opinion pieces, non-scientific editorials, unpublished manuscripts, conference proceedings that do not meet journal article standards, or purely technical articles in the field of information technology that discuss only algorithms, encryption, attack detection, or network engineering without linking them to dimensions of governance, operational resilience, institutional accountability, or market implications. Establishing explicit criteria from the outset is a crucial requirement to ensure that a systematic review does not devolve into a loose narrative review (Page et al., 2021; Paul et al., 2021; Sauer & Seuring, 2023).

The screening procedure is carried out in stages. All records retrieved from the databases are first exported to a reference management tool for automatic deduplication, then manually re-verified to avoid erroneous deletions. The next stage involves screening of titles and abstracts based on the established inclusion and exclusion criteria, followed by an assessment of full-text eligibility for articles still considered potential candidates. At the full-text assessment stage, selection was based not only on the presence of keywords, but primarily on conceptual relevance, depth of analysis, and the article's alignment with the study's main focus: the relationship between cyber governance, operational resilience, and market confidence in financial institutions. This phased procedure aligns with systematic review practices that emphasise transparency in selection decisions and a rationale for exclusions (Page et al., 2021).

Following selection, eligible articles were extracted using a structured data extraction sheet. The information recorded includes author names, year of publication, journal, research focus, institutional context, jurisdiction where relevant, key concepts, methodological orientation, main arguments or findings, governance implications, dimensions of operational resilience, as well as references to trust, credibility, reputation, market confidence, or systemic stability. This extraction is carried out to enable systematic comparison between studies without imposing homogeneity on a literature that is naturally multidisciplinary. Within the framework of a systematic review, standardised data extraction is crucial for maintaining the consistency of the synthesis and reducing interpretative bias arising from unstructured reading (Brignardello-Petersen et al., 2025; Flemming & Noyes, 2021).

The analysis was conducted in two phases. The first phase was a thematic synthesis to identify recurring patterns, clusters of concepts, and analytical tensions within the literature corpus. Through this process, articles were grouped by themes such as cyber governance architecture, board and senior management oversight, cyber risk accountability, critical function continuity, recovery capacity, crisis preparedness, reliance on third parties, stakeholder trust, and regulatory alignment.

Thematic synthesis was chosen because this method preserves the richness of meaning found in qualitative and conceptual studies, whilst providing a systematic analytical structure. The second layer is normative analysis, which evaluates how the literature defines what financial institutions and regulators should do in managing cyber risk and building operational resilience, as well as whether existing conceptualisations are adequate to support market confidence. Thus, the normative analysis in this article does not stop at description, but moves towards an evaluation of the adequacy, coherence, and institutional implications of the arguments found in the literature (Ayre & McCaffery, 2022; Flemming & Noyes, 2021; Smith & Miller, 2025).

Methodologically, the combination of a systematic literature review and a normative analysis provides a strong justification for the aims of this article. A systematic review enables the structured mapping and synthesis of a fragmented field, whilst a normative analysis allows for a more incisive assessment of conceptual adequacy, the distribution of governance responsibilities, institutional legitimacy, and the regulatory direction that should be pursued. Therefore, this methodology section is designed not only to demonstrate how the literature was gathered, but also to explain how it was transformed into a foundation for an academically accountable evaluation (Lim et al., 2022; Sauer & Seuring, 2023; Smith & Miller, 2025).

3. RESULT

3.1. Study Selection and Descriptive Profile of the Literature

The application of the selection procedures resulted in a literature pool that was compiled in a gradual and rigorous manner. During the identification stage, a total of 709 records were obtained from all the sources used. Following an automated deduplication process and manual verification, 176 records were removed due to duplication, leaving 533 unique records for the title and abstract screening stage. Of these, 378 records were excluded as they were irrelevant to the research focus, primarily because they addressed cybersecurity from a technical perspective without addressing governance dimensions, operational resilience, institutional implications, or consequences for market confidence. Consequently, 155 reports were selected for full-text retrieval, though 8 of these could not be obtained adequately. The full-text assessment stage was then carried out on these 147 articles.

Table 1. Identification stage under PRISMA 2020

Source of records	Records identified
Scopus	214
Web of Science Core Collection	158
ScienceDirect	96
SpringerLink	72
Wiley Online Library	41
Taylor and Francis Online	34
Emerald Insight	23
Google Scholar, supplementary search	44
Backward citation tracking	11
Forward citation tracking	9
Manual reference list and journal-site checks	7
Total records identified	**709**

Table 2. Screening stage under PRISMA 2020

Screening item	Number
Total records identified	709
Duplicate records removed	176
Records after deduplication	**533**
Records screened by title and abstract	533
Records excluded at title and abstract stage	378
Reports sought for retrieval	**155**
Reports not retrieved	8
Full-text reports assessed for eligibility	**147**

During the selection phase, 97 articles were excluded following a thorough review as they did not meet the substantive research criteria. The most common reason for exclusion was an overly technical focus that was not related to cyber governance, operational resilience, regulation, or market confidence. Other articles were excluded because they did not focus on financial institutions or financial infrastructure, were not peer-reviewed journal articles, did not provide adequate discussion of governance or operational resilience, were duplicate publications, or lacked sufficient bibliographic integrity. Once all these stages were complete, 50 studies were included in the systematic synthesis and normative analysis.

Table 3. Eligibility stage under PRISMA 2020, full-text exclusions

Reason for exclusion after full-text review	Number
Purely technical cybersecurity focus, with no governance, resilience, regulatory, or market dimension	31
Not focused on financial institutions, financial regulation, or financial infrastructures	24
Not a peer-reviewed journal article	15
No substantive analysis of cyber governance or operational resilience	13
Overlapping or duplicate publication of the same study	5
Incomplete full text or insufficient bibliographic integrity	4
Non-English full text	3
Outside the operative date window	2
Total full-text exclusions	**97**

Table 4. Included studies under PRISMA 2020, final thematic composition

Dominant analytical focus of included studies	Number
Cyber governance, board oversight, and accountability	15
Operational resilience, continuity of critical functions, and recovery capability	12
Market confidence, trust, disclosure, and reputational effects	10
Cyber risk as financial stability or systemic risk	7
Regulatory architecture, DORA, supervision, and third-party risk	6
Total included studies	**50**

Descriptively, the final dataset shows that the literature is not evenly distributed, but is concentrated in a few key areas of discussion. Most studies address cyber governance, board oversight, management accountability, and cyber risk disclosure. The next group focuses on operational resilience, the continuity of critical functions, recovery capabilities, and preparedness for disruptions. A number of other studies examine market confidence through reputation, stakeholder trust, market reactions, and the relevance of information disclosure to investors. The remainder relate to cyber risk as a financial stability issue, as well as regulatory architecture, particularly concerning digital operational resilience, third-party governance, and supervisory coordination.

The profile of the collected literature also indicates that this field is highly interdisciplinary. The articles included are drawn from journals in the fields of finance, banking, governance, information systems, public policy, business ethics, regulation, and cybersecurity. In terms of approach, the analysed literature is not homogeneous: there are empirical studies based on archives and corporate disclosures, event studies analysing market responses to cyber incidents, systematic reviews, as well as conceptual articles and legal-regulatory analyses. This diversity highlights that the relationship between cyber governance, operational resilience, and market confidence cannot be adequately understood through a single discipline alone.

In terms of temporal development, publications in this corpus increased significantly between 2022 and 2025, signalling a growing academic focus on cyber risk as an institutional and regulatory issue, rather than merely a technological problem. Geographically, these studies are largely centred on the contexts of the United States, the United Kingdom, and Europe, though they are beginning to encompass other jurisdictions and emerging markets. The findings of this profile are significant as they indicate that the analysed literature has developed sufficiently to permit a mature thematic synthesis, yet still exhibits strong conceptual fragmentation between governance, operational resilience, and market confidence. On this basis, the synthesis in the following sections aims not only to map out themes, but also to assess the coherence and adequacy of the relationships between these three dimensions within the context of financial institutions.

3.2. Descriptive Mapping of the Literature

The literature review in this study describes a rapidly evolving field that remains conceptually uneven. In the majority of academic studies, cyber governance is not formulated as a mature institutional theory concerning digital financial intermediaries; rather, the concept is generally operationalised through board oversight, senior management accountability, governance-related disclosures, the characteristics of audit and risk committees, and formal processes for identifying, reporting, and monitoring cyber risk exposure. In this configuration, cyber governance is primarily treated as a matter of oversight, transparency, and control, particularly in listed companies and regulated entities, rather than as a broader governance architecture linking strategic direction, operational capacity, and institutional credibility under digital pressures. Consequently, the literature is relatively robust in identifying governance mechanisms and disclosure practices, yet underdeveloped in conceptualising cyber governance as an integrated institutional capability within the financial sector.

Operational resilience is generally treated in more concrete terms than cyber governance, but also within a more functionally limited framework. The dominant view defines operational resilience in terms of the continuity of critical services, the ability to withstand disruptions, the capacity to recover from cyber and technological incidents, and the management of dependencies involving digital infrastructure and third-party providers. In banking and other systemic financial environments, this concept is usually articulated through operational continuity, incident response, recovery planning, and infrastructure dependencies, rather than through broader questions of institutional trust or market legitimacy. Recent regulatory reviews, particularly those related to the EU Digital Operational Resilience Act, further reinforce this orientation by emphasising ICT risk management, testing, reporting, supervisory coordination, and third-party concentration risk. Consequently, operational resilience has been relatively well defined as a functional and regulatory

category, yet it is still more frequently treated as a construct of continuity and compliance rather than as an institutional attribute that builds trust.

Conversely, market confidence is the core concept that has been least explicitly analysed among the three. In most of the literature, this concept emerges indirectly through related constructs such as firm value, abnormal stock returns, the informativeness of disclosures, investor willingness to invest, reputational damage, or user trust in digital financial services. Studies conducted within the context of capital markets and corporate finance indicate that cyber risk is priced in, successful cyber attacks can damage shareholder value and reputation, and disclosure choices can shape investor assessments. In fintech-oriented research, the same issues emerge through the terminology of trust, security, and adoption, yet are rarely linked back to cyber governance or operational resilience within an integrated institutional framework. The descriptive pattern is clear: the literature devotes substantial attention to the impact of cyber incidents on trust-related outcomes, yet far less attention is paid to market trust as an explicit integrative category linking governance arrangements, resilience capacity, and the credibility of financial institutions under cyber pressure.

The sectoral distribution of the literature is also uneven. Banking is the dominant institutional context, particularly in studies addressing disclosure, governance oversight, operational resilience, performance, stability, and supervisory expectations. A second major strand focuses on listed companies and the capital markets environment, where the analytical focus lies on cyber risk disclosure, pricing, firm valuation, and investor responses. Fintech constitutes a smaller yet distinct strand, where cybersecurity relates more directly to customer trust, perceptions of security, and adoption behaviour. Payment systems and the broader financial market infrastructure feature primarily in studies on systemic cyber risk and network amplification, rather than within the established governance–resilience–trust literature for these sectors. Meanwhile, insurance remains on the periphery and is more frequently examined through the lens of the sustainability of the cyber insurance market and the limits of risk transfer, rather than through in-depth analysis of cyber governance within insurance institutions themselves.

This distribution is reflected in the dominant analytical orientations within the field. The majority of studies are structured around risk management, disclosure, compliance, cyber security controls, regulatory responses, operational continuity, or business continuity logic, whilst far fewer studies explicitly link these orientations to market trust as a result of systemic or institutional reproduction. Research focusing on disclosure stands out prominently, both in the accounting and governance literature and in specialised banking studies, indicating that transparency has become one of the primary empirical windows through which cyber risk is observed and evaluated. At the same time, resilience studies and financial stability studies largely run along separate tracks, with the former emphasising continuity and recovery, whilst the latter focuses on contagion, amplification, and systemic vulnerability. Descriptively, therefore, the literature does not develop these three core concepts in a balanced manner: cyber governance and operational resilience are more prominent, although they often reside within the silos of different disciplines, whilst market confidence is more frequently implied than directly theorised. This uneven conceptual distribution provides the necessary foundation for subsequent thematic synthesis and normative analysis, which must address not only what the literature covers, but also how its internal fragmentation shapes the current state of knowledge.

4. DISCUSSION

4.1. The Integration of Cyber Governance and Operational Resilience in Financial Institutions

a. Reaffirming the Core Argument of the Study

The key findings of this study confirm that cyber risk within financial institutions can no longer be adequately understood as a standalone technical disruption, but rather as an institutional issue that touches upon governance design, accountability, the continuity of critical functions, and the maintenance of trust in digitally mediated markets. This direction is consistent with a body of literature demonstrating that cyber vulnerabilities increase alongside digital interdependence,

operational exposure, and the potential for systemic effects on key nodes of the financial system, whilst institutional responses to such risks span issues of disclosure, oversight, resilience, and market reaction. Consequently, cyber governance and operational resilience are better understood not as separate, parallel domains, but as two mutually reinforcing institutional capacities in maintaining market confidence.

This argument also explains why the previous literature appears strong in parts but weak in its integration. Within the reviewed corpus, governance studies largely address board oversight, committee structures, and disclosure; resilience studies emphasise continuity, recovery, and dependency management; whilst market studies capture the impact of cyber attacks through firm value, reputational pressure, abnormal returns, and investor response. However, these three strands tend to develop within distinct analytical silos, meaning that the relationship between governance arrangements, resilience capacity, and the formation of market confidence has not yet been adequately synthesised. Consequently, the contribution of this discussion is not merely to affirm that all three are relevant, but to demonstrate that the institutional interaction between cyber governance and operational resilience constitutes an analytical prerequisite for understanding market confidence in financial institutions.

b. Cyber Governance as the Institutional Architecture of Accountability

The literature reviewed indicates that cyber governance is most frequently operationalised through board oversight, senior management accountability, risk governance, disclosure practices, committee structures, and formal monitoring processes. A number of studies show that the quality of cyber risk disclosure is related to governance characteristics, whether through board gender diversity, board effectiveness, the IT expertise of the audit committee, the existence of a cyber committee, or board structures that influence the scope and quality of disclosure (Alodat et al., 2025; Chen et al., 2022; Gao & Calderon, 2025; Héroux & Fortin, 2022; Opuni-Frimpong et al., 2024; Radu & Smaili, 2022; Smaili et al., 2023a; Zheng et al., 2025). At the same time, studies on disclosure indicate that cyber disclosure remains frequently generic, uneven, and only becomes more specific when triggered by regulatory pressure, risk exposure, or reporting incentives (Calderon & Gao, 2022; Cheong et al., 2021; Gao et al., 2020; Héroux & Fortin, 2022; Jiang et al., 2022; López et al., 2025). These findings suggest that cyber governance, in empirical practice, has not yet fully emerged as a mature institutional theory, but is already clearly emerging as the primary arena where cyber accountability is shaped and accounted for.

However, a more nuanced interpretation demands that cyber governance not be reduced to a mere compliance tool or administrative control mechanism. In the context of financial institutions, cyber governance is more appropriately understood as an institutional architecture of accountability—that is, an institutional framework that determines who bears responsibility for cyber risks, how risks are prioritised at the strategic level, how escalation and reporting are conducted, and how institutional credibility is established in the eyes of regulators, investors, counterparties, and service users. The conceptual framework proposed by Harel and Carmeli (2025) clarifies that cyber risk must be positioned as a strategic governance issue, not a subordinate technical issue. From this perspective, disclosure is not an end in itself, but rather a manifestation of deeper accountability. Consequently, without credible governance, operational resilience loses its strategic direction: an institution may possess technical procedures and operational responses, but lacks a clear centre of accountability to set priorities, coordinate functions, and maintain reliability under pressure.

c. Operational Resilience as the Functional Condition of Institutional Reliability

Unlike cyber governance, which is more frequently discussed through the lens of oversight and disclosure, operational resilience is presented in the literature in a more concrete and functional manner. It is generally understood in terms of the continuity of critical services, response capability, recovery capacity, crisis preparedness, and the management of digital and third-party dependencies. Studies on the disclosure of bank resilience indicate that this area remains under-reported and

uneven, whilst regulatory analysis of DORA places resilience within the framework of ICT risk management, testing, incident reporting, supervisory coordination, and oversight of third-party concentration risk (Buttigieg & Zimmermann, 2024; Jančiūtė, 2025; Leo, 2020). Other studies indicate that resilience and better cyber policies are associated with stronger operational risk management, post-attack recovery capabilities, and reduced vulnerability to liquidity shocks in the banking sector (Abaidoo & Agyapong, 2026; Baatwah et al., 2025; Bruno et al., 2025). This confirms that resilience in financial institutions is not an abstract attribute, but rather a measurable operational capacity in the continuity of critical functions amidst disruptions.

Nevertheless, the literature often still narrows operational resilience down to issues of continuity and compliance. Such an interpretation is too narrow for the financial sector, as financial institutions are not only expected to continue internal processes but also to maintain the reliability of intermediation, payment, custody, and settlement functions that underpin market confidence. Therefore, operational resilience is more appropriately positioned as a functional condition of institutional reliability. The market does not assess security merely by the absence of incidents, but by an institution's ability to withstand, recover, preserve critical functions, and manage disruption without losing credibility. In this sense, resilience is not merely the ability to recover after a disruption, but the capacity to uphold the institutional commitment that core services remain reliable when the system is under pressure.

d. How Cyber Governance and Operational Resilience Interact

The most important synthesis of this study is that cyber governance and operational resilience are mutually reinforcing, rather than two separate agendas. In the governance literature, governance is established through board oversight, senior management accountability, the expertise of audit and cyber committees, the quality of disclosure, and a monitoring structure that treats cyber risk as a strategic institutional issue, rather than merely a technical or administrative compliance issue (Chen et al., 2022; Gao et al., 2020; Harel & Carmeli, 2025; Opuni-Frimpong et al., 2024; Radu & Smaili, 2022; Zheng et al., 2025). On the other hand, the resilience literature indicates that an institution's capacity to maintain the continuity of critical services, respond to incidents, restore operations, and manage digital and third-party dependencies is at the core of operational resilience in financial institutions (Abaidoo & Agyapong, 2026; Bruno et al., 2025; Buttigieg & Zimmermann, 2024; Jančiūtė, 2025; Leo, 2020). Thus, the relationship between the two is causal-institutional: governance establishes risk priorities, lines of accountability, escalation procedures, and oversight; whilst resilience translates these orientations into tangible operational capabilities that enable the institution to maintain critical functions under pressure. Consequently, the clearer an institution's accountability architecture, the greater the likelihood that resilience will be built in a targeted, tested, and accountable manner.

From this, it is evident that governance without resilience tends to be formalistic. An institution may possess committee structures, policies, and disclosures that appear adequate, yet still fail to safeguard core operations when a cyber disruption actually occurs. Conversely, resilience without governance tends to be technocratic and institutionally weak: technical capacity may be available, but it is not embedded within a clear structure of strategic accountability, making it difficult to direct, audit, and use as a basis for the institution's credibility. This pattern aligns with findings that stronger governance is associated with better disclosure quality, more effective risk oversight, lower breach risk, and stronger banking performance; whilst greater resilience is associated with the ability to withstand post-attack impacts, strengthened management of operational risk, and reduced vulnerability to liquidity shocks and systemic pressures (Abaidoo & Agyapong, 2026; Baatwah et al., 2025; Bruno et al., 2025; Chen et al., 2022; Ismail, 2024; Opuni-Frimpong et al., 2024). In the context of highly digitalised and interconnected financial institutions, reliability under disruption does not stem from technology alone, nor from disclosure alone, but from the convergence of institutional accountability and operational capability.

It is at this point that the bridge to market confidence becomes clear: the market is more likely to maintain confidence in institutions that not only recognise cyber risks, but also demonstrate

that these risks are managed within a credible governance framework and translated into tangible, sustainable operational capacity relevant to the stability of financial functions (Anand et al., 2026; Eisenbach et al., 2022a; Florackis et al., 2023; Uddin et al., 2020).

e. Market Confidence as an Institutional Outcome, Not a Residual Effect

The reviewed literature indicates that market confidence most often emerges indirectly, rather than as a clearly defined core concept. It is inferred through reputational effects, abnormal returns, stock market reactions, disclosure credibility, investor response, and trust in digital financial services. Event studies and market analyses indicate that data theft, announcements of data breaches, major cyberattacks, and news of cyberattacks can reduce market value, damage reputation, and trigger negative investor reactions, with the intensity influenced by timing, the severity of the incident, and the credibility of the information source (Chang et al., 2020; Florackis et al., 2023a; Foerderer & Schuetz, 2022; Makridis, 2021; Martins et al., 2025; Muktadir-Al-Mukit & Ali, 2025; Peng et al., 2023). In the context of fintech and digital banking, trust and security also emerge as core determinants of the adoption of digital financial services; thus, cyber threats impact not only capital market valuations but also user trust in digitised financial services (Cele & Kwenda, 2025; Jafri et al., 2023; Okat et al., 2025).

Nevertheless, this article argues that market confidence should not be treated as a residual effect following an incident. It is more accurately understood as an institutional outcome of credible governance and effective resilience. Reputation, investor sentiment, firm value, legitimacy, and disclosure effects may indeed function as indicators or manifestations, but none of these are identical to market confidence itself. In the context of financial institutions, market confidence refers to the belief that an institution is capable of maintaining the continuity of intermediation, the reliability of payment and settlement functions, the capacity to manage disruption, and the credibility of the institutional response when a cyber incident occurs. Thus, market confidence is both ex ante and ex post: it may be eroded following an incident, but its foundation is established beforehand through governance arrangements and resilience capacity that lead the institution to be deemed trustworthy even before an attack actually occurs.

4.2. Toward an Integrated Institutional Framework and Normative Priorities for Financial Institutions

Based on the synthesis in the previous subsection, the main issue in the literature is no longer merely a lack of discussion regarding cyber governance, operational resilience, or market confidence in isolation, but rather the absence of an evaluative framework that adequately links all three at the institutional level. The governance literature has extensively addressed variations in board oversight, the quality of disclosure, the role of committees, and the influence of leadership characteristics on an organisation's response to cyber risks, whilst the resilience literature has clarified the importance of continuity, recovery, preparedness, and dependency management in safeguarding critical financial services. On the other hand, the market literature has demonstrated that cyber risks affect investor assessments, corporate value, reputation, and confidence in digital financial services. However, these three strands are still more frequently interpreted as parallel explanatory frameworks rather than as a single, mutually reinforcing institutional architecture (Buttigieg & Zimmermann, 2024; Florackis et al., 2023; Harel & Carmeli, 2025; Liu & Babar, 2024; Radu & Smaili, 2022; Smaili et al., 2023). Consequently, the conceptual contribution required at this stage is not a repetition of the descriptions of each domain, but rather the development of a framework explaining how the quality of governance influences operational capacity, and how both together form a sound foundation for market confidence.

Within this framework, financial institutions must be understood not merely as entities managing cyber risk, but as institutions that must be capable of translating strategic oversight into observable operational reliability. This means that the quality of cyber governance can no longer be evaluated solely on the basis of the existence of formal structures, the extent of disclosure, or symbolic compliance; it must be assessed by its ability to set priorities, clarify responsibilities, and

compel the organisation to link board-level decisions with the protection of critical functions. By the same logic, operational resilience cannot be adequately assessed by the mere existence of recovery plans or policy language, but rather by whether the institution truly possesses the capacity to maintain core functions, manage digital dependencies, and limit damage when disruptions occur. It is at this point that market confidence acquires a more definitive institutional meaning: it is not merely a psychological market response, but an assessment of whether an institution possesses sufficient governance and operational capacity to remain trustworthy under digital pressure (Abaidoo & Agyapong, 2026; Anand et al., 2026; Chen et al., 2022; Gao & Calderon, 2025; Jančiūtė, 2025; Opuni-Frimpong et al., 2024).

The normative implications for financial institutions are therefore quite clear. It is no longer sufficient for institutions to treat cyber risk merely as a matter for the technology, compliance, or periodic reporting units. What is needed instead is genuine board-level accountability, cross-functional governance integration, and escalation mechanisms that ensure cyber issues are treated as matters of institutional continuity, not merely as technical control issues. At the operational level, normative priorities must focus on resilience testing of critical functions, oversight of third-party dependencies, recovery credibility, and communication capacity during incidents, as it is precisely in these areas that the difference between formal compliance and substantive institutional preparedness becomes most apparent. Findings regarding the importance of IT expertise within audit committees, the role of cyber committees, the adequacy of DORA architecture, and the value of post-attack resilience demonstrate that institutional preparedness demands more than mere documentation; it demands capabilities that can be demonstrated in practice (Baatwah et al., 2025; Bruno et al., 2025; Buttigieg & Zimmermann, 2024; Chen et al., 2022; Zheng et al., 2025).

From this perspective, a more relevant measure for assessing financial institutions is no longer whether they possess cyber controls, but whether they are capable of institutionalising the relationship between oversight, response, recovery, and market credibility into a coherent framework. Consequently, visible institutional preparedness must be treated as a normative standard of greater importance than mere formal compliance. A trustworthy institution is not merely one that discloses risks, but one that can demonstrate that its governance fosters organisational discipline, that its resilience safeguards core functions, and that both together underpin the confidence of investors, users, counterparties, and authorities when digital disruptions occur. Thus, this subsection presents the synthesis findings not as a descriptive conclusion, but as a basis for assessing the institutional adequacy of financial institutions in maintaining market confidence amidst deepening digital interdependence (Cumming et al., 2026; Eisenbach et al., 2022; Florackis et al., 2023; Uddin et al., 2020).

5. CONCLUSION

This study This study concludes that cyber risk in financial institutions should no longer be understood as a standalone technical disruption, but rather as an institutional issue that touches upon governance design, the distribution of accountability, the continuity of critical functions, and the maintenance of trust in a digitalised market. Through a systematic literature review combined with normative analysis, this article demonstrates that the relationship between cyber governance, operational resilience, and market confidence constitutes the core of an issue that has not yet been adequately synthesised, as the literature has developed in silos of governance, resilience, and market-based studies. On this basis, this article asserts that cyber governance is more appropriately understood as an architecture of accountability, operational resilience as a capability for continuity and recovery, and market confidence as a trust-based institutional outcome.

Conceptually, the main contribution of this article lies in the reorganisation of fragmented literature into a single integrated institutional framework. This framework demonstrates that market confidence should not be reduced to a post-incident market reaction, but must be interpreted as an institutional outcome shaped ex ante through credible governance and effective operational capacity, and then re-evaluated ex post when digital disruptions actually occur. Thus, the resilience of financial institutions under cyber pressure does not stem solely from technology, nor is it sufficient

to rely on disclosure or formal compliance alone; rather, it arises from the convergence of strategic oversight, accountability discipline, protection of core functions, recovery capacity, and the credibility of institutional responses.

Normatively, these findings demand that financial institutions no longer treat cyber risk solely as a matter for the technology unit or administrative compliance. What is required is genuine board-level accountability, cross-functional governance integration, resilience testing of critical functions, oversight of third-party dependencies, credibility in recovery, and the capacity for reassuring communication when incidents occur. Consequently, a more relevant evaluation standard is no longer whether an institution possesses formal cyber controls, but rather whether it possesses sufficient governance and operational capacity to safeguard critical functions and maintain market confidence amidst deepening digital interdependence. In this sense, this article positions visible institutional preparedness as a more substantive normative measure than formal compliance alone.

REFERENCES

Abaidoo, R., & Agyapong, E. K. (2026). Operational resilience, macroeconomic uncertainty and exposure to liquidity shocks among US commercial banks. *Studies in Economics and Finance*, 1–22. https://doi.org/10.1108/SEF-05-2025-0362

Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2025). Board characteristics and cybersecurity disclosure: Evidence from the UK. *Electronic Commerce Research*, *25*, 4717–4735. https://doi.org/10.1007/s10660-024-09867-w

Anand, K., Duley, C., & Gai, P. (2026). *Cybersecurity and financial stability*.

Ayre, J., & McCaffery, K. J. (2022). Research note: Thematic analysis in qualitative research. *Journal of Physiotherapy*, *68*(1), 76–79. https://doi.org/10.1016/j.jphys.2021.11.002

Baatwah, S. R., Asiri, M., Bajaher, M. S., Alyafai, A., & Baajajah, S. (2025). Thriving post-cyberattacks: The power of control, disclosure, and IT maturity. *Electronic Commerce Research*, *26*, 1705–1743. https://doi.org/10.1007/s10660-025-09958-2

Brignardello-Petersen, R., Santesso, N., & Guyatt, G. H. (2025). Systematic reviews of the literature: An introduction to current methods. *American Journal of Epidemiology*, *194*(2), 536–542. https://doi.org/10.1093/aje/kwae232

Bruno, E., Pistolesi, F., & Teti, E. (2025). *Cybersecurity policy, ESG and operational risk: a virtuous relationship to improve banks' performance*.

Buttigieg, C. P., & Zimmermann, B. B. (2024). *The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision*.

Calderon, T. G., & Gao, L. (2022). *Changes in corporate cybersecurity risk disclosures after SEC comment letters*.

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Chang, K. C., Gao, Y. K., & Lee, S. C. (2020). The effect of data theft on a firm's short-term and long-term market value. *Mathematics*, *8*(5), 808. https://doi.org/10.3390/math8050808

Chen, C., Hartmann, C., & Gottfried, A. (2022). *The Impact of Audit Committee IT Expertise on Data Breaches*.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). *Classifying the Contents of Cybersecurity Risk Disclosure through Textual Analysis and Factor Analysis*.

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis*, *65*, 101386. https://doi.org/10.1016/j.irfa.2019.101386

Cumming, D., Nguyen, M., Pham, A. V, & Samarasinghe, A. (2026). *Banking system stability: a global analysis of cybercrime laws*.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802–826. https://doi.org/10.1016/j.jfineco.2021.10.007

Flemming, K., & Noyes, J. (2021). Qualitative evidence synthesis: Where are we at? *International Journal of Qualitative Methods*, *20*, 1609406921993276. https://doi.org/10.1177/1609406921993276

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023a). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: A matter of

timing? *Management Science*, *68*(10), 7298–7322. https://doi.org/10.1287/mnsc.2021.4264
Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy*, *54*, 107376. https://doi.org/10.1016/j.jaccpubpol.2025.107376
Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468
Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567–594. https://doi.org/10.2307/25750692
Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683–714. https://doi.org/10.1080/07421222.2018.1451962
Harel, Y., & Carmeli, A. (2025). *A strategic cybersecurity oversight framework: A board's imperative*.
Héroux, S., & Fortin, A. (2022). *Board of directors' attributes and aspects of cybersecurity disclosure*.
Ismail, E. A. A. (2024). *The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region*.
Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2023). A systematic literature review of the role of trust and security on Fintech adoption in banking. *Heliyon*, *10*(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980
Jančiūtė, L. (2025). Cybersecurity in the financial sector and the quantum-safe cryptography transition: In search of a precautionary approach in the EU Digital Operational Resilience Act framework. *International Cybersecurity Law Review*, *6*(2), 145–154. https://doi.org/10.1365/s43439-025-00135-7
Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems*, *36*(1), 151–180. https://doi.org/10.2308/ISYS-2020-067
Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019
Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, *8*(4), 128. https://doi.org/10.3390/risks8040128
Lim, W. M., Kumar, S., & Ali, F. (2022). Advancing knowledge through literature reviews: What, why, and how to contribute. *The Service Industries Journal*, *42*(7--8), 481–513. https://doi.org/10.1080/02642069.2022.2047941
Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, *51*(1), 62–92. https://doi.org/10.1177/03128962241293658
López, F. A., Jara-Sarrúa, L., Morales-Parada, F., & Palos-Sánchez, P. R. (2025). Cybersecurity disclosure in the financial sector: An examination of the influence of incident exposure, governance practices, and regulatory context. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-025-10081-5
Makridis, C. A. (2021). *Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018*.
Martins, A. M., Moutinho, N., & Cró, S. (2025). Stock market effects of major cyber-attacks: Evidence for breached and cybersecurity listed firms. *Journal of Banking Regulation*, *26*, 868–877. https://doi.org/10.1057/s41261-025-00293-y
Muktadir-Al-Mukit, D., & Ali, M. H. (2025). *The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study*.
Okat, D., Paaso, M., & Pursiainen, V. (2025). Trust in Traditional Finance and Consumer Fintech Adoption. *The Review of Corporate Finance Studies*, *14*(2), 408–438. https://doi.org/10.1093/rcfs/cfae011
Opuni-Frimpong, J., Adefunso Dzorka, M., & Boadi, I. (2024). Governance's role in bank performance: Cybersecurity committee assessment. *Journal of Financial Reporting and Accounting*, *23*(2), 788–810. https://doi.org/10.1108/JFRA-12-2023-0774
Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & McKenzie, J. E. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ*, *372*, n160. https://doi.org/10.1136/bmj.n160
Paul, J., Merchant, A., Dwivedi, Y. K., & Rose, G. M. (2021). Writing an impactful review article: What do we know and what do we need to know? *Journal of Business Research*, *133*, 337–340. https://doi.org/10.1016/j.jbusres.2021.05.005
Peng, J., Zhang, H., Mao, J., & Xu, S. (2023). *Repeated data breaches and firm value*.

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics*, *177*, 351–374. https://doi.org/10.1007/s10551-020-04717-9

Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., & Koffel, J. B. (2021). {PRISMA-S}: An extension to the {PRISMA} statement for reporting literature searches in systematic reviews. *Systematic Reviews*, *10*(1), 39. https://doi.org/10.1186/s13643-020-01542-z

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*, 146–154. https://doi.org/10.1016/j.irfa.2017.01.001

Sauer, P. C., & Seuring, S. (2023). How to conduct systematic literature reviews in management research: A guide in 6 steps and 14 decisions. *Review of Managerial Science*, *17*, 1899–1933. https://doi.org/10.1007/s11846-023-00668-3

Schmitz, J., & Leoni, G. (2019). Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. *Australian Accounting Review*, *29*(2), 331–342. https://doi.org/https://doi.org/10.1111/auar.12286

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, *27*(4), 1049–1071. https://doi.org/10.1007/s10997-022-09637-6

Smith, M., & Miller, S. (2025). Technology, institutions and regulation: Towards a normative theory. *AI & Society*, *40*, 1007–1017. https://doi.org/10.1007/s00146-023-01803-0

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020a). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*. https://doi.org/10.1057/s41283-020-00063-2

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020b). *Cybersecurity hazards and financial system vulnerability: A synthesis of literature*.

Zheng, G., Xia, Z., He, F., & Xiao, Z. (2025). *The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk*.