



Influence of Operational and Cyber Risk on Risk Governance in Digital Banking

Janne Hillary¹

¹ Politeknik Negeri Pontianak, Pontianak, Indonesia

Abstract

Article history:

Received: July 20, 2025

Revised: September 21, 2025

Accepted: October 25, 2025

Published: December 30, 2025

Keywords:

Banking regulation,

Cyber risk,

Digital banking,

Operational risk,

Risk governance.

Identifier:

Zera Open

Page: 148-163

<https://zeraopen.com/journal/amos>

The rapid digitalization of banking services has significantly transformed operational processes while simultaneously increasing exposure to operational and cyber risks. System disruptions, data breaches, and cyberattacks have emerged as critical threats that may undermine banks' governance structures and financial stability. This study conceptually examines the influence of operational and cyber risk on risk governance in digital banking environments. Drawing on recent academic literature and regulatory guidance published over the last five years, the paper synthesizes key insights on how operational failures and cyber incidents affect governance frameworks, internal controls, and supervisory oversight in banks. The analysis highlights that digital banking intensifies the interdependence between operational risk management and cyber resilience, requiring more integrated governance approaches. Effective risk governance is shown to depend on clear accountability structures, robust internal control systems, and alignment with regulatory expectations related to technology and security risk. The study contributes to the banking risk literature by providing a structured conceptual perspective on the governance implications of operational and cyber risk in increasingly digitalized banking systems. The findings offer relevant insights for regulators and banking practitioners seeking to strengthen risk governance frameworks in the face of growing digital and cyber-related threats.



1. Introduction

The rapid expansion of digital banking has fundamentally transformed how financial institutions deliver services, manage operations, and interact with customers. While digitalization has improved efficiency and accessibility, it has simultaneously increased banks' exposure to operational and cyber risks. System failures, technology outages, data breaches, and cyberattacks now represent material sources of risk that can disrupt critical banking functions, undermine customer trust, and threaten financial stability. Consequently, regulators and supervisors increasingly recognize operational and cyber risks as integral components of overall banking risk management frameworks (Basel Committee on Banking Supervision, 2021).

Operational risk has long been associated with failures in internal processes, human error, and system deficiencies (Moosa, 2021). In digital banking environments, these traditional sources of operational risk are amplified by greater reliance on complex information technology infrastructures and third-party service providers (Bank for International Settlements, 2021). Digital transformation further increases the likelihood of operational disruptions with potentially systemic implications, particularly when banking services depend on interconnected digital platforms (Basel Committee on Banking Supervision, 2022).

Cyber risk, which encompasses threats related to unauthorized access, data theft, and cyberattacks on banking systems, has emerged as a critical dimension of operational risk in the digital era (Caralli et al., 2020). The increasing frequency and sophistication of cyber incidents have intensified regulatory attention on cyber resilience and security governance in financial institutions (International Monetary

Fund, 2022). These developments highlight the growing importance of integrating cyber risk into broader operational risk management frameworks (Kopp et al., 2020).

Risk governance plays a central role in determining how banks identify, assess, and respond to operational and cyber risks (Renn, 2020). It encompasses the structures, processes, and accountability mechanisms through which risk-related decisions are made and overseen at managerial and board levels (Nyman & Ormerod, 2020). In digital banking contexts, governance challenges are intensified by technological complexity and evolving regulatory expectations (European Central Bank, 2022).

Weaknesses in risk governance can exacerbate the impact of operational and cyber risk events by limiting effective oversight and response mechanisms (Gatzert & Schmit, 2020). Conversely, strong governance frameworks can enhance resilience by ensuring that operational and cyber risks are systematically integrated into enterprise-wide risk management processes (World Bank, 2023).

Despite growing scholarly and regulatory interest in operational and cyber risks, the literature remains fragmented regarding their combined governance implications in digital banking environments (Schinasi, 2021). Existing studies often address cybersecurity or operational risk in isolation, leaving a gap in integrated conceptual analysis of how these risks jointly influence governance structures (Sullivan & McConnell, 2022).

Accordingly, this study aims to conceptually examine the influence of operational and cyber risk on risk governance in digital banking. By synthesizing recent academic research and regulatory guidance, the study seeks to develop an

integrated understanding of how digitalization reshapes risk profiles and governance challenges in banking. The analysis contributes to the literature by providing a conceptual foundation for understanding the governance implications of operational and cyber risk in digital banking environments.

2. Literature Review

2.1. Operational Risk in Digital Banking

Operational risk represents a fundamental category of banking risk associated with failures in internal processes, systems, human factors, and external events (Moosa, 2021). The expansion of digital banking has significantly transformed the nature of operational risk by increasing reliance on complex technological infrastructures and third-party service providers (Bank for International Settlements, 2020). This transformation has intensified the scale and speed at which operational disruptions can occur, particularly within highly interconnected digital financial systems (Basel Committee on Banking Supervision, 2021).

Recent studies suggest that operational risk in digital environments is increasingly driven by technology-related failures rather than traditional process inefficiencies (Power, 2021). The integration of digital platforms into core banking functions has created new vulnerabilities that may lead to systemic disruptions when not adequately managed (Zetsche et al., 2020). As a result, operational risk management frameworks are required to evolve toward more technology-oriented approaches that emphasize resilience and continuity (Basel Committee on Banking Supervision, 2022).

2.2. Cyber Risk as a Dimension of Operational Risk

Cyber risk has emerged as a critical extension of operational risk, encompassing threats such as cyberattacks, data breaches, and unauthorized access to financial systems (Caralli et al., 2020). Unlike traditional operational risks, cyber risk is characterized by its dynamic nature and potential for rapid propagation across institutions and markets (Kopp et al., 2020). This characteristic increases the likelihood that cyber incidents may generate systemic consequences beyond individual banks (International Monetary Fund, 2021).

Empirical and policy-oriented research indicates that cyber risk events can significantly undermine financial stability by disrupting services and eroding market confidence (International Monetary Fund, 2022). The increasing frequency and sophistication of cyber threats have led regulators to emphasize cyber resilience as a core component of banking supervision frameworks (World Bank, 2023). Consequently, cyber risk is no longer treated as a purely technical issue but as a strategic governance concern within financial institutions (McConnell & Blacker, 2021).

2.3. Risk Governance and Supervisory Expectations

Risk governance defines the institutional structures and processes through which banks manage and oversee risk-related decisions (Renn, 2020). It plays a crucial role in ensuring that operational and cyber risks are effectively identified, assessed, and controlled within banking organizations (Gatzert & Schmit, 2020). In digital banking contexts, governance frameworks are required to adapt to increased complexity, uncertainty, and technological dependency (Nyman & Ormerod, 2020).

Regulatory bodies have increasingly emphasized the importance of strong governance structures in enhancing operational resilience and accountability (European Central Bank, 2022). Effective risk governance requires clear allocation of responsibilities, active board involvement, and robust internal control mechanisms (Basel Committee on Banking Supervision, 2021). Furthermore, the literature highlights that governance effectiveness depends on the integration of risk management practices across organizational levels and functional areas (Schinasi, 2021).

2.4. Digitalization, Governance Challenges, and Systemic Implications

Digital transformation introduces significant governance challenges by increasing organizational complexity and accelerating innovation cycles (Zetzsche et al., 2020). These developments may create gaps between existing governance structures and emerging risk profiles, particularly when institutions fail to adapt their oversight mechanisms (World Bank, 2022). The lack of coordination between business, technology, and risk management functions can weaken the effectiveness of risk governance frameworks (Sullivan & McConnell, 2022).

From a systemic perspective, digital banking increases the interconnectedness of financial institutions, thereby amplifying the potential impact of operational and cyber disruptions (Sahay et al., 2020). Large-scale cyber incidents or operational failures may therefore pose risks to financial stability, requiring coordinated regulatory responses and information-sharing mechanisms (International Monetary Fund, 2022). These conditions highlight the need for governance frameworks that

align firm-level risk management with broader macroprudential objectives (Schinasi, 2021).

2.5. Research Gap and Conceptual Contribution

Despite the growing body of literature on operational and cyber risk, existing studies often examine these risks in isolation rather than as interconnected governance challenges (Eling & Wirfs, 2020). This fragmented approach limits the ability to fully understand how digitalization reshapes risk governance structures in banking (Power, 2021). Moreover, limited research provides an integrated conceptual framework that combines regulatory perspectives with academic insights on risk governance (Nyman & Ormerod, 2020).

Accordingly, this study addresses this gap by synthesizing recent academic and regulatory literature into a unified conceptual analysis of operational and cyber risk governance in digital banking. The study adopts a systematic literature review approach to integrate insights across disciplines and to provide a structured foundation for future research and policy development in banking risk management.

3. Methods

This study employs a qualitative research design based on a systematic literature review (SLR) to examine the influence of operational and cyber risk on risk governance in digital banking environments. The SLR approach is adopted to ensure a transparent, structured, and replicable synthesis of existing academic and regulatory literature, while avoiding the use of original empirical data. This methodological choice aligns with the conceptual objective of the study and is appropriate for

integrating insights from banking risk management, information systems governance, and financial regulation.

The literature review process followed a structured three-stage procedure consisting of identification, screening, and inclusion. During the identification stage, relevant publications were retrieved through systematic searches in Google Scholar using predefined keywords, including “operational risk,” “cyber risk,” “risk governance,” “digital banking,” and “financial regulation.” These keywords were selected to capture studies addressing both traditional operational risk issues and emerging cyber-related challenges in digital banking contexts. To ensure relevance and timeliness, the search was restricted to publications released between 2020 and 2024.

In the screening stage, retrieved studies were evaluated based on predefined inclusion and exclusion criteria. Peer-reviewed journal articles and institutional reports from internationally recognized regulatory bodies were included to ensure academic rigor and policy relevance. Studies focusing exclusively on technical cybersecurity solutions without discussion of governance, regulatory, or risk management implications were excluded. This screening process ensured that the final body of literature directly addressed the governance dimension of operational and cyber risk.

The final stage involved qualitative content analysis of the selected literature. Each study was systematically reviewed and coded using a thematic analysis approach. The coding process focused on identifying recurring themes related to governance structures, accountability mechanisms, supervisory expectations, and

risk integration practices in digital banking. The analysis was structured around three core analytical dimensions: (1) the impact of operational risk on governance frameworks, (2) the role of cyber risk in shaping governance and oversight, and (3) the integration of operational and cyber risk within enterprise-wide risk governance structures.

By synthesizing findings across these dimensions, the study develops an integrated conceptual understanding of how operational and cyber risks influence risk governance in digital banking environments. This qualitative synthesis provides a structured foundation for discussing regulatory and managerial implications, while also identifying areas for future research and policy development related to digital risk governance in the banking sector.

4. Results

This section presents the key insights derived from the systematic literature review regarding the influence of operational and cyber risk on risk governance in digital banking (Basel Committee on Banking Supervision, 2021). Rather than reporting statistical results, the analysis synthesizes recurring themes and conceptual patterns identified across recent academic and regulatory sources (Power, 2021). The discussion is structured around the analytical dimensions specified in the Method section and situates the findings within contemporary debates on banking governance and digital resilience (Schinasi, 2021).

4.1. Key Themes Identified from the Literature

The reviewed literature consistently emphasizes that digitalization reshapes the nature of operational risk while simultaneously elevating cyber risk to a central governance concern (World Bank, 2023). As banks rely increasingly on digital platforms, cloud services, and third-party providers, operational disruptions and cyber incidents are shown to have broader organizational and reputational consequences (Moosa, 2021). Risk governance frameworks are therefore required to evolve in order to address these interconnected risks more effectively (Gatzert & Schmit, 2020).

Table 1. Key Themes in Operational and Cyber Risk Governance in Digital Banking

Analytical Dimension	Key Insights from Literature	Implications for Systemic Risk
Operational risk exposure	Digital systems amplify process and system failures	Stronger internal controls required
Cyber risk intensity	Increased frequency and sophistication of cyber threats	Enhanced cyber oversight mechanisms
Risk interdependence	Operational and cyber risks are closely intertwined	Integrated risk governance needed
Governance structures	Board-level involvement is increasingly emphasized	Clear accountability and oversight
Regulatory expectations	Supervisors stress operational resilience	Alignment with supervisory guidance

The table indicates that the governance impact of digitalization extends beyond technical risk controls and requires strategic oversight at the organizational level.

4.2. Influence of Operational Risk on Risk Governance

The literature suggests that operational risk in digital banking environments exerts significant influence on governance arrangements (Basel Committee on Banking Supervision, 2022). Operational disruptions such as system outages or failures in third-party services can expose weaknesses in decision-making structures, escalation procedures, and accountability mechanisms (Bank for International Settlements, 2021). As a result, governance frameworks that were previously adequate in traditional banking contexts may prove insufficient in digitally intensive environments (Nyman & Ormerod, 2020).

Studies emphasize that effective risk governance requires clear delineation of roles and responsibilities across business units, technology functions, and risk management teams (Renn, 2020). Operational risk events often highlight gaps in coordination and communication, prompting regulators to demand stronger governance structures that ensure timely risk identification and response (International Monetary Fund, 2022). From this perspective, operational risk acts as a catalyst for strengthening governance practices in digital banking institutions (Schinasi, 2021).

4.3. Cyber Risk and Governance Challenges

Cyber risk presents distinct governance challenges due to its dynamic and evolving nature (Caralli et al., 2020). Unlike traditional operational risk events, cyber incidents can emerge rapidly, propagate across systems, and affect multiple institutions simultaneously (Kopp et al., 2020). The literature highlights that cyber risk governance requires continuous oversight, specialized expertise, and

active involvement from senior management and boards (McConnell & Blacker, 2021).

The findings indicate that banks with fragmented governance arrangements may struggle to manage cyber risk effectively, particularly when responsibility for cybersecurity is dispersed across organizational units (Sullivan & McConnell, 2022). In contrast, integrated governance frameworks that embed cyber risk within enterprise-wide risk management processes are better positioned to enhance resilience and regulatory compliance (World Bank, 2022).

Table 2 provides a conceptual comparison of governance approaches to operational and cyber risk in digital banking.

Table 2. Conceptual Comparison of Risk Governance Approaches

Aspect	Conventional Stress Testing	Integrated Risk Stress Testing
Risk focus	Separate risk categories	Integrated operational–cyber risk
Board involvement	Limited technology oversight	Active digital risk oversight
Accountability	Fragmented responsibilities	Clear ownership and escalation
Regulatory alignment	Compliance-oriented	Resilience- and governance-oriented
Risk response	Reactive	Proactive and preventive

The comparison illustrates that digital risk–integrated governance frameworks offer greater capacity to address the complexities of operational and cyber risk in modern banking environments.

5. Discussion

The synthesized findings suggest that operational and cyber risks are not merely technical challenges, but governance issues that shape how banks manage risk in digital contexts. Weak governance structures can amplify the impact of operational failures and cyber incidents, while strong governance frameworks can enhance resilience and regulatory credibility.

The discussion aligns with broader regulatory perspectives that view governance as a cornerstone of operational resilience. Digital banking intensifies the need for governance models that are adaptive, integrated, and forward-looking. Accordingly, the results support a conceptual view in which effective risk governance serves as the primary mechanism through which banks translate operational and cyber risk management into sustainable digital resilience.

6. Conclusion

This study conceptually examines the influence of operational and cyber risk on risk governance in digital banking environments through a systematic literature review and qualitative synthesis of recent academic and regulatory sources. The analysis highlights that digitalization fundamentally reshapes banks' operational risk profiles while elevating cyber risk to a central governance concern. Operational disruptions and cyber incidents are no longer isolated technical events, but governance challenges that directly affect organizational resilience, regulatory compliance, and financial stability.

The findings suggest that effective risk governance plays a decisive role in determining how banks respond to operational and cyber risks in increasingly digitalized contexts. Governance frameworks characterized by clear accountability, strong board-level oversight, and integration of technology and cyber risk into enterprise-wide risk management are better positioned to mitigate the impact of digital risk events. Conversely, fragmented governance structures may amplify vulnerabilities and undermine banks' ability to manage complex and rapidly evolving threats.

From a regulatory perspective, the study underscores the growing emphasis on governance as a cornerstone of operational resilience. Supervisory authorities increasingly expect banks to demonstrate that operational and cyber risks are systematically embedded within governance structures, supported by robust internal controls and oversight mechanisms. Accordingly, operational and cyber risk management should be viewed not merely as compliance requirements, but as strategic components of sound risk governance in digital banking.

This research contributes to the banking risk literature by providing an integrated conceptual perspective on operational risk, cyber risk, and governance in digital banking. It offers relevant insights for regulators and practitioners seeking to strengthen governance frameworks in response to digital transformation. Future research may extend this conceptual analysis by empirically examining governance practices across banking systems or by exploring emerging digital risks and their regulatory implications.

References

- Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements.
- Basel Committee on Banking Supervision. (2021). *Sound practices: Implications of fintech developments for banks and bank supervisors*. Bank for International Settlements.
- Basel Committee on Banking Supervision. (2022). *Operational risk: Revisions to the principles*. Bank for International Settlements.
- Bank for International Settlements. (2020). *Sound practices: Implications of fintech developments for banks*. BIS.
- Bank for International Settlements. (2021). *Operational resilience and cyber risk*. BIS Quarterly Review.
- Bank for International Settlements. (2022). *Principles for financial market infrastructures and operational resilience*. BIS.
- Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2020). *Cyber resilience: Engineering risk management*. Addison-Wesley.
- Eling, M., & Wirfs, J. H. (2020). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109–1119.
- European Central Bank. (2022). *Supervisory expectations on ICT and cyber risk management*. ECB Banking Supervision.
- Gatzert, N., & Schmit, J. (2020). Supporting strategic decisions with enterprise risk management. *European Journal of Finance*, 26(10), 1001–1020.
- International Monetary Fund. (2021). *Global financial stability report: Preempting a legacy of vulnerabilities*. IMF.

- International Monetary Fund. (2022). *Global financial stability report: Financial stability risks from cyber threats*. IMF.
- Kopp, E., Kaffenberger, L., & Wilson, C. (2020). Cyber risk, market failures, and financial stability. *IMF Working Paper*.
- McConnell, P., & Blacker, K. (2021). Managing cyber risk in financial institutions. *Journal of Banking Regulation*, 22(4), 323–337.
- Moosa, I. (2021). *Operational risk management*. Palgrave Macmillan.
- Nyman, R., & Ormerod, P. (2020). Rethinking risk governance. *Journal of Risk Research*, 23(9), 1143–1156.
- Power, M. (2021). *The risk management of everything* (2nd ed.). Profile Books.
- Renn, O. (2020). Risk governance: Coping with uncertainty in a complex world. *Earthscan*.
- Sahay, R., von Allmen, U. E., Lahreche, A., Khera, P., Ogawa, S., Bazarbash, M., & Beaton, K. (2020). *The promise of fintech*. IMF.
- Schinasi, G. (2021). Preserving financial stability. *Journal of Financial Regulation and Compliance*, 29(3), 205–218.
- Sullivan, K., & McConnell, P. (2022). Cyber risk governance in banking. *Journal of Financial Regulation and Compliance*, 30(2), 159–175.
- World Bank. (2022). *Global financial development report: Finance for an equitable recovery*. World Bank Publications.
- World Bank. (2023). *Cybersecurity risk management for financial institutions*. World Bank.
- Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. (2020). From fintech to techfin. *New York University Journal of Law & Business*, 16(1), 1–47.