Journal of Sciences, Computing and Applied Engineering Research (JSCAER), Vol. 2, No.1, pp. 48-52
Published Online (https://jcaes.net) , January 17, 2026 by SciTech Network Press ISSN: 3092-8648

Safest Banks: A Scientific Literature Review on Financial Stability and Risk Management Practices

Emughedi Oghu
Department of Computer Science, Lead City University , Ibadan, Nigeria
Corresponding Author: Email Address:emughedi.oghu@pgstudent.lcu.edu.ng

Received: 2 November 2025; Revised: 12 January2026; Accepted: 14 January 2025; Published: 17 January 2026

Abstract The concept of a "safe bank" has become a central concern for policymakers, investors, and the public following the 2008 Global Financial Crisis and subsequent periods of economic uncertainty. This paper presents a comprehensive literature review that synthesizes the key themes and findings from academic research on bank safety. In particular, the concept through three interconnected lenses: the measurement of financial stability, the internal risk management architectures of banks, and the external framework of governance and regulation is analysed. The review identifies that safety is not a singular attribute but a multi-dimensional construct, defined by a robust capital base, a resilient and integrated risk management culture, strong corporate governance, and effective prudential regulation. Key metrics such as capital adequacy ratios (CET1), the Z-score, and stress test results are discussed alongside qualitative factors like risk culture. The literature converges on the importance of Enterprise Risk Management (ERM) frameworks and the pivotal role of Basel III in elevating industry standards. Finally, this paper identifies critical gaps in the current literature, particularly concerning the integration of climate-related financial risks, the systemic implications of FinTech disruption, and the influence of organizational culture, offering a roadmap for future scholarly inquiry.

Keywords: Bank Safety, Financial Stability, Risk Management, Basel III, Corporate Governance, Systemic Risk, Literature Review.

1. Introduction

The stability of the banking sector is a cornerstone of modern economic prosperity. The 2008 Global Financial Crisis (GFC) starkly demonstrated that the failure of seemingly large and sophisticated financial institutions can trigger profound economic and social turmoil, leading to a "Great Recession" (Gorton, 2012). In the aftermath, the academic and regulatory communities have intensively focused on understanding, defining, and measuring what constitutes a "safe bank." The recent shocks from the COVID-19 pandemic, geopolitical instability, and high-profile bank failures (e.g., Silicon Valley Bank, Credit Suisse) have further underscored the dynamic and evolving nature of banking risks and the imperative of financial resilience.

The primary contribution of this paper is the synthesis of a vast and multi-disciplinary body of literature spanning finance, economics, management, and regulation. By organizing the research into distinct but interrelated themes, this review provides a holistic framework for understanding bank safety. It moves beyond a simple list of metrics to explore the underlying practices and systemic structures that foster stability.

The structure of this paper is as follows. Section 2 presents the bank safety overview and examines the various quantitative with qualitative methods used to define and measure bank safety. Section 3 delves into the core engine of safety: internal risk management practices, from enterprise-wide frameworks to the management of specific risk types. Section 4 analyzes the external scaffold provided by corporate governance and the post-GFC regulatory paradigm. Section 5 offers a discussion that synthesizes these

themes and identifies critical gaps in the literature. Finally, Section 6 concludes with a summary of findings and proposes directions for future research.

2. A Detailed overview Bank Safety Measure and Literature

This literature review seeks to answer the central research question: Based on existing academic literature, what are the defining characteristics, frameworks, and metrics that constitute a "safe bank" in the contemporary financial environment?

2.1 Process and Measure of Bank Safety:

The concept of "safety" is inherently multidimensional. The literature approaches its measurement through a combination of backward-looking accounting data, forward-looking market-based indicators, and regulatory assessments.Peihani (2022) examined the organization of cyber-risk governance within Canadian banking institutions and concluded that the traditional Basel operational-risk framework fails to adequately address cyber threats. He proposed that banks, including the Royal Bank of Canada, should transition toward resilience-oriented systems focused on dynamic oversight, rapid post-incident learning, ongoing simulation testing, and inter-bank coordination. The study identified multifactor authentication (MFA), employee training, real-time network surveillance, and cooperation between regulatory bodies and banks as vital aspects of effective cyber-risk management.

Eijkelenboom (2021) analyzed the annual reports of publicly listed Dutch companies, including major banks, to assess the depth of cybersecurity disclosures. His results indicated that while many institutions reference cybersecurity, only a minority provide specific details regarding their defensive strategies. He argued that limited disclosure about endpoint detection, intrusion monitoring, board involvement, and vendor resilience weakens both governance transparency and operational security. The author emphasized that comprehensive reporting enhances accountability and fosters stakeholder confidence in cyber governance.

Ahnert (2023) developed a theoretical framework conceptualizing cyber-attack risk in banking as a systemic externality, where a single breach can spread across interconnected financial networks. His model demonstrated that large institutions have an economic incentive to invest in cybersecurity not merely for individual protection but to prevent contagion within the wider banking ecosystem. The findings imply that regulation plays an essential role by setting minimum standards for resilience and encouraging coordinated defense strategies that safeguard overall financial stability.

Doing et al. (2024) carried out an empirical assessment of phishing-reporting behavior among staff and clients in a European bank. Their findings revealed that the ease and immediacy of reporting determine user participation in identifying phishing threats. The introduction of “Report Phish” buttons and automated feedback systems markedly improved reporting rates. Furthermore, integrating user reports into the Security Operations Center (SOC) enhanced detection precision and shortened response time. The authors concluded that motivating and rewarding users for rapid reporting complements technical defenses, collectively strengthening institutional resilience.

Anand et al. (2023) explored the relationship between cybersecurity investment and macro-financial stability across several countries. The authors found that enhanced cybersecurity spending produces positive externalities that extend beyond individual banks, reducing systemic vulnerability. Their analysis showed that incidents within one institution can cascade through shared third-party service providers, increasing sector-wide risk. They recommended the creation of coordinated information-sharing platforms and cross-border regulatory cooperation to minimize the spread of cyber contagion.

Kanyongo and Wadesango (2025) investigated the impact of cybersecurity practices on risk reduction in commercial banks in Zimbabwe and South Africa. They identified multifactor authentication, regular cybersecurity audits, and staff awareness training as key defenses against breaches. Their study also noted that regulatory oversight and executive-level accountability improve organizational resilience. For developing economies, they recommended cost-effective approaches such as endpoint protection, SMS-based alerts, and user education as practical measures to prevent cyber incidents.

Fedele (2024) conducted a mixed-method study focusing on phishing victims and their financial implications for banks. The study showed that customers with limited digital literacy are more prone to online fraud. Financial institutions implementing adaptive MFA, device fingerprinting, and behavioral scoring mechanisms reported up to 60% fewer losses. Additionally, AI-driven transaction monitoring systems improved fraud prediction. The author advocated the integration of behavioral biometrics to enhance online banking authentication and strengthen customer protection.

Jimmy (2024) synthesized global evidence on cyber threats in online banking, identifying ransomware, phishing, and DDoS attacks as dominant challenges. He proposed a layered security approach combining data encryption, Security Information and Event Management (SIEM) tools, and regular penetration testing. The study emphasized that continuous monitoring and public awareness programs are crucial for maintaining robust cybersecurity. Adaptive authentication was found to be highly effective in reducing fraudulent activities across online platforms. Sulong (2025) analyzed data from 150 international banks spanning two decades to determine the influence of cybersecurity investments on risk-taking behavior. His econometric findings indicated that banks with formal cybersecurity departments and regular red-team simulations exhibited fewer operational losses. The results underscored that robust cybersecurity systems act as deterrents to reckless financial behavior and promote long-term institutional stability.

Burda et al. (2024) examined how employee motivation affects the reporting of phishing attempts in financial institutions. They discovered that gamification strategies—such as leaderboards and recognition programs—enhanced participation and accuracy in threat reporting. Banks linking reporting metrics to performance evaluation observed quicker response times and reduced repeated attacks. The study recommended that institutions adopt simulation-based training and reward programs to build a culture of cybersecurity vigilance. Alqahtani et al. (2023) investigated the adoption of blockchain technology in Islamic banking as a means of enhancing cybersecurity. The researchers demonstrated that blockchain's decentralized architecture ensures transaction immutability and transparency, significantly reducing fraud and insider threats. Smart contracts were also found to improve compliance with Islamic finance principles. The study concluded that blockchain provides both technological and ethical reinforcement of cybersecurity within Islamic financial systems.

Rahman and Nasir (2023) analyzed the application of artificial intelligence (AI) for detecting cyber intrusions in Southeast Asian banks. They found that using supervised models for known threats alongside unsupervised algorithms for anomalies achieved a 94% detection accuracy. Their results emphasized the importance of continuous model retraining and cross-institutional collaboration to keep pace with evolving threat landscapes. The integration of AI-driven defense systems proved effective in preventing data exfiltration and insider breaches.

Mensah (2025) evaluated cybersecurity governance structures across African banking institutions and found that inadequate coordination and limited funding were major barriers to resilience. He proposed a comprehensive framework that merges policy development, human capital management, and technological investment under a unified cybersecurity governance unit. Banks adopting this model reported fewer security incidents and improved strategic oversight of cyber risks.

Jakovljević (2022) explored cybersecurity perceptions within the Serbian banking sector, finding that many customers underestimate the severity of digital threats. Despite the increasing sophistication of attacks on web and mobile banking, awareness among users remained low. The author stressed that banks must enhance both technical infrastructure and customer education to address human vulnerabilities and build cyber resilience.

Best, Krumov, and Bacivarov (2019) conducted a comparative study of security risks in the banking sector and proposed a model for mitigating data-leakage threats. They identified malware, insider abuse, and phishing as key attack vectors. The study highlighted the importance of access control management, logging mechanisms, and segregation of duties as preventive tools. Implementing visualization systems for data leakage further enhanced early threat detection and internal monitoring.

Gowda and Gowda (2022) argued for a shift from traditional perimeter-based defense to the "Zero Trust" security model in modern banking. This approach requires continuous verification of every user and device, regardless of location, thereby eliminating assumptions of inherent safety within internal networks. They advocated adaptive authentication and breach-assumption policies to strengthen systemic resilience against insider and external threats.

Miya and Joseph (2025) traced the progression of cybersecurity strategies in the banking sector over the past twenty years. Their research demonstrated how institutions evolved from basic antivirus tools to comprehensive security operations centers (SOCs), advanced threat-hunting programs, and board-level cyber governance structures. They concluded that institutional learning and cultural adaptation play a greater role in resilience than isolated technical solutions.

Yıldırım (2024) assessed the growing importance of cybersecurity amid rising digital transaction volumes in global banking. The study found that institutions increasingly rely on strong authentication, end-to-end encryption, and automated incident response to preserve customer trust. Yıldırım stressed the need for banks to synchronize their cybersecurity strategies with both operational demands and regulatory requirements to sustain long-term resilience.

Elsayed et al. (2024) examined the relationship between cybersecurity disclosures and financial performance among banks in the MENA region. The findings indicated that banks providing detailed

disclosures—particularly concerning board-level oversight, IT governance, and risk management—exhibited stronger financial performance. Transparent reporting was seen as a signal of robust internal control and proactive risk mitigation, reinforcing stakeholder confidence.

Metibemu (2025) investigated cybersecurity practices in digital-only banks operating within cashless economies. The study revealed that these institutions have evolved beyond conventional antivirus tools to adopt multilayered security architectures encompassing fraud analytics, compliance with anti-money-laundering regulations, and scenario-based threat modeling. Metibemu emphasized that digital-only banks, lacking physical infrastructure, must invest more intensively in real-time detection and response capabilities to maintain operational integrity. Shown in table 1 is a summary literature review on safety banks over time. Despite a robust body of work, several critical gaps remain, representing rich avenues for further research work.

Table 1: A Literature Review compact on safety Banks in recent time

Author & Year	**Name of Bank**	**Cybersecurity Measures**	**Last Known Attack & Preventive Measures to curb future occurrence**
Doing et al. (2024)	European bank	Phishing reporting, Security operation Center (SOC) integration	Reduced phishing recurrence; proactive reporting and SOC-based monitoring
Anand et al. (2023)	Global banks	Information sharing, regulation	Prevented systemic contagion via cooperative resilience testing
Kanyongo & Wadesango (2025)	African banks	MFA, cyber audits	Fewer fraud incidents; periodic training and cyber hygiene
Fedele (2024)	Global banks	AI detection, biometrics	Lower financial losses; predictive transaction monitoring
Jimmy (2024)	Global banks	Encryption, SIEM	Prevented DDoS recurrence; enhanced customer awareness programs
Sulong (2025)	Global banks	Red teaming, Security operation Center (SOC) maturity	Reduced risk-taking losses; investment in dedicated cyber teams
Burda et al. (2024)	European Bank	Gamified phishing reporting	Reduced repeat attacks; gamification of reporting improved vigilance
Alqahtani et al. (2023)	Islamic banks	Blockchain, smart contracts	No insider fraud; blockchain ensured immutability and transparency
Rahman & Nasir (2023)	Asian banks	AI intrusion detection	Prevented data exfiltration; hybrid supervised-unsupervised models
Mensah (2025)	African banks	Governance reform, audits	Reduced breach frequency; cross-departmental coordination
Peihani (2022)	Royal Bank of Canada	MFA, real-time monitoring, staff training	No recent breach documented; resilience testing and

			regulatory collaboration
Eijkelenboom (2021)	Dutch listed banks	EDR, board oversight, vendor resilience	No breach disclosed; enhanced disclosure and board monitoring
Ahnert (2023)	Large banks (theoretical)	Systemic defense investment, coordination	No attack case; regulatory stress testing and minimum defense standards
Jakovljević (2022)	Serbian banks	Mobile/web security, user awareness	None reported; improved customer awareness programs
Best et al. (2019)	Banking sector	Access control, data-leakage visualization	None specific; implemented logging and segregation controls
Gowda & Gowda (2022)	Banking institutions	Zero Trust, adaptive authentication	None specific; implemented continuous verification frameworks
Miya & Joseph (2025)	Global banks	SOCs, layered governance	None specific; promoted institutional cyber learning culture
Yıldırım (2024)	Digital transaction banks	Strong authentication, continuous monitoring	None reported; improved alignment with regulatory and operational needs
Elsayed et al. (2024)	MENA region banks	Board oversight, IT committee governance	No incidents disclosed; improved cyber disclosure and transparency
Metibemu (2025)	Digital-only banks	Fraud analytics, real-time monitoring	No breach recorded; scaled layered fraud detection systems

2.2 Quantitative Metrics

(i) Capital Adequacy: The most widely cited measure of a bank's safety cushion is its capital. The Basel Committee on Banking Supervision (BCBS) established the Basel Accords, with Basel III representing the current global standard. A key metric is the Common Equity Tier 1 (CET1) ratio, which measures a bank's core equity capital against its risk-weighted assets. A higher CET1 ratio signifies a greater ability to absorb unexpected losses without failing. Studies consistently find a strong inverse relationship between bank capitalization and the probability of failure or distress (Berger & Bouwens, 2009).

(ii) Insolvency Risk (Z-Score): A classic measure in the literature is the Z-score, which quantifies the number of standard deviations a bank's return on assets (ROA) must fall below its expected value before equity is wiped out (Boyd & Graham, 1986). A higher Z-score indicates a lower probability of insolvency. While powerful for its simplicity, the Z-score has been critiqued for its assumption of normally distributed returns and its reliance on historical accounting data, which may not capture future risks (Laeven & Levine, 2009).

(iii) Asset Quality (Non-Performing Loans - NPLs): The ratio of non-performing loans to total loans is a direct indicator of credit risk exposure and asset quality. High levels of NPLs can erode profitability and consume capital, signaling underlying weaknesses in a bank's lending practices and economic outlook (Klein & Weill, 2019).

(iv) Market-Based Indicators: Financial markets offer real-time assessments of bank safety. Credit ratings from agencies like Moody's and S&P provide a holistic view of creditworthiness. Market-based measures such as Credit Default Swap (CDS) spreads and stock price volatility are also used as forward-looking indicators of perceived risk (Flannery & Kwan, 2005). However, these can be noisy and subject to market sentiment, potentially over- or under-reacting to fundamental conditions.

2.3 Qualitative Dimensions

Beyond hard numbers, the literature recognizes qualitative factors such as depositor confidence, institutional reputation, and management quality as crucial components of safety (Goddard et al., 2009). These are difficult to quantify directly but are often reflected in the quantitative metrics over time and are central to regulatory supervision.

3. Methodology: Risk Management as the Core Engine of Safety

Metrics are outcomes, while risk management is the process that produces them. The literature overwhelmingly points to sophisticated and integrated risk management as the primary differentiator between safe and risky banks.

3.1 The Rise of Enterprise Risk Management (ERM)

The GFC exposed the failures of siloed risk management, where different risk types (credit, market, operational) were managed in isolation. The contemporary literature champions the ERM framework, promoted by bodies like the Committee of Sponsoring Organizations of the Treadway Commission (COSO). ERM provides a holistic, top-down approach to identifying, assessing, managing, and monitoring all material risks across an organization (Nocco & Stulz, 2006). It aligns risk management with strategic objectives and establishes a clear "risk appetite" defined by the board and senior management.

3.2 Management of Key Risk Types

(i) Credit Risk: As the traditional core of banking, sound credit risk management remains paramount. This involves rigorous underwriting standards, portfolio diversification, continuous monitoring of borrower financial health, and prudent provisioning for expected losses (Jacobson et al., 2005). Recent literature explores the use of artificial intelligence and machine learning to enhance credit scoring models and detect early warning signals of default.

(ii) Liquidity Risk: The GFC highlighted liquidity risk—the inability to meet short-term obligations—as a "silent killer." Northern Rock's 2007 run is a canonical example. In response, Basel III introduced two key, non-risk-based liquidity metrics: the Liquidity Coverage Ratio (LCR), ensuring banks hold enough high-quality liquid assets to survive a 30-day stress scenario, and the Net Stable Funding Ratio (NSFR), promoting longer-term, more stable funding structures (BCBS, 2013).

(iii) Market and Operational Risk: For banks with significant trading activities, market risk management (e.g., Value-at-Risk models) is critical. Operational risk, encompassing failures in internal processes, people, and systems, has gained prominence with the rise of digital banking and cyber threats. The literature increasingly focuses on cyber resilience, business continuity planning, and the role of RegTech in automating compliance and monitoring operational risks (Bamberger, 2020).

4. The External Scaffold: Governance and Regulation

A bank's safety is not determined in a vacuum. It is profoundly shaped by its governance structure and the regulatory environment in which it operates.

4.1 Corporate Governance

The literature establishes a strong link between weak corporate governance and excessive risk-taking. Key factors include:

(a) **Board Structure:** The effectiveness of the board of directors, its independence, financial expertise, and the presence of a dedicated, standalone risk committee are critical for overseeing risk management (Pathan, 2009).
(b) **Executive Compensation:** Compensation structures that heavily reward short-term performance can incentivize excessive risk-taking. The literature highlights the importance of "say-on-pay" initiatives, clawback provisions, and the use of long-term incentive instruments (e.g., deferred stock) to align executive actions with long-term stability (Bebchuk & Spamann, 2010).

4.2 The Post-GFC Regulatory Paradigm

The post-2008 era has been defined by a significant tightening of prudential regulation.

(i) **Basel III:** Beyond higher capital and liquidity requirements, Basel III introduced a leverage ratio (a non-risk-based backstop), capital buffers (counter-cyclical and systemic), and more stringent rules for systemically important financial institutions (SIFIs). The literature credits Basel III with making the banking system more resilient, though some debate exists about its impact on lending and economic growth (Borio & Disyatat, 2010).
(ii) **Stress Testing:** Supervisory stress testing has become a cornerstone of modern regulation. Programs like the Comprehensive Capital Analysis and Review (CCAR) in the U.S. and the EBA stress tests in the EU subject banks to severe hypothetical economic scenarios to assess their capital adequacy under duress. Hirtle (2018) argues that stress testing has not only improved banks' capital planning but also increased market discipline by making risk information more transparent.
(iii) **Resolution Regimes:** To combat the "too-big-to-fail" problem, regulators have developed "living wills" and resolution regimes that aim to allow for the orderly failure of a large bank without taxpayer bailouts and without causing systemic contagion.

5. Discussion and Finding

The reviewed literature converges on a clear judgment: **bank safety is an emergent property of a triad of strong internal risk management, robust corporate governance, and effective external regulation as revealed in Fig.1.** One pillar cannot compensate for a fundamental weakness in another. A well-capitalized bank with poor governance may still fail, while a bank with strong governance but inadequate regulation may be unable to withstand a systemic shock.

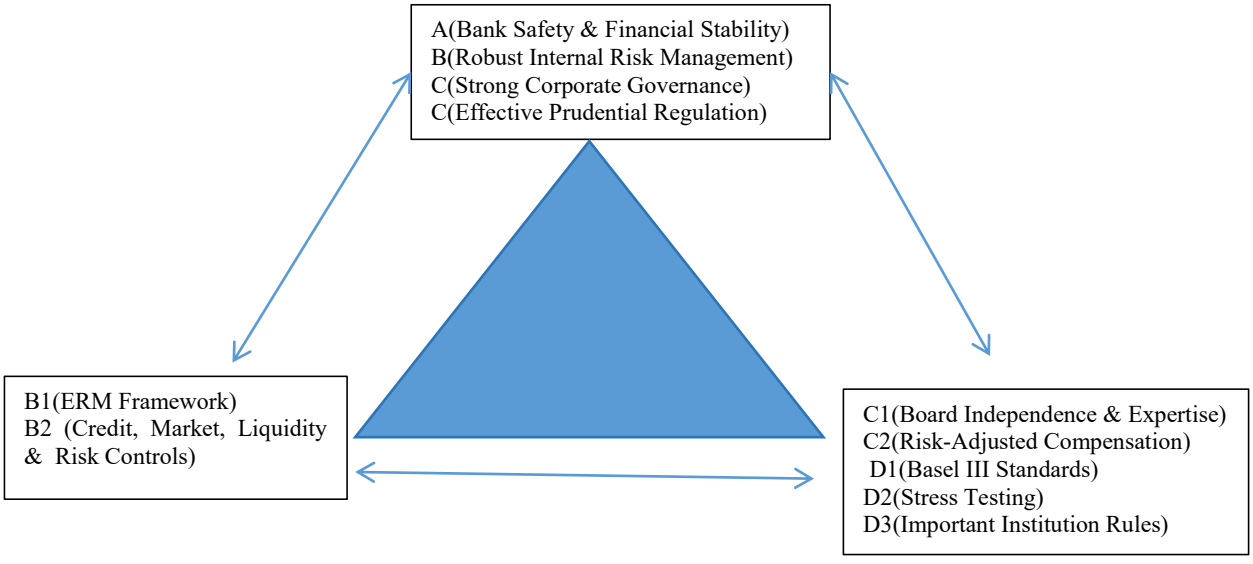

Fig. 1: Conceptual Triad of Bank Safety graph TD

(i) **Climate-Related Financial Risks:** While the literature is emerging, there is no consensus on how to effectively model and incorporate the physical and transition risks of climate change into traditional risk management frameworks and prudential supervision. The long-term horizon and unprecedented nature of these challenges pose significant methodological difficulties.
(ii) **FinTech and BigTech Disruption:** The rise of non-bank financial institutions, from neobanks to BigTech firms offering financial services, challenges the traditional bank-centric model of safety. Research is needed to understand whether these entities create new, less visible systemic risks, and how regulatory frameworks should adapt to this evolving landscape (FSB, 2019).
(iii) **The Role of Culture and Ethics:** Quantitative models dominate the literature, yet many risk management failures stem from poor organizational culture, ethical lapses, and groupthink. A deeper, more qualitative investigation of the "soft" factors that underpin a strong risk culture—leadership tone, psychological safety, and incentive alignment—is needed.
(iv) **Cross-Cultural and Emerging Market Contexts:** The vast majority of foundational research on bank safety is centered on developed economies (U.S. and Europe). More comparative studies are required to understand how the determinants of safety may differ in emerging markets, where institutional quality, market structure, and regulatory enforcement can vary significantly.

6. Conclusion and Future Research Directions

This literature review has synthesized the academic understanding of what makes a bank "safe." The evidence suggests that safety is a dynamic and holistic construct, moving far beyond a simple assessment of capital levels. It is the product of a virtuous cycle: effective regulation forces better governance and risk management, which in turn leads to stronger financial metrics and greater market confidence. The modern "safest bank" is characterized by a deeply embedded ERM culture, overseen by an expert and independent board, and operating within a regulatory regime that emphasizes forward-looking resilience through stress testing and stringent capital and liquidity standards.

The quest for bank safety is a perpetual race against innovation and evolving risks. The future of banking will be shaped by digitalization, climate change, and geopolitical shifts. Consequently, future research must address the identified gaps. Priorities should include developing robust frameworks for climate risk stress testing, analyzing the systemic footprint of the FinTech ecosystem, and creating methodologies to measure and improve risk culture. By pursuing these avenues, the academic community can continue to provide the evidence base needed to build a more resilient and safer global financial system.

References

Aderemi, K., & Olamide, A. (2020). Digital watermarking for document security in financial institutions. *Journal of Information Security Research, 5*(3), 82–95.
Ahnert, T. (2023). Cyber risk and security investment. Bank of Canada Research Paper.
Alqahtani, H., Khan, R., & Rashid, M. (2023). Blockchain-based cybersecurity framework for Islamic banks. Journal of Financial Innovation and Technology, 9(2), 114–130.
Anand, K., Gai, P., & Kapadia, S. (2023). Cybersecurity and financial stability. SUERF Policy Brief No. 343.
Best, M., Krumov, L., & Bacivarov, I. C. (2019). Cyber Security in Banking Sector. International Journal of Information Security and Cybercrime, 8(2).
Burda, P., Doing, A.-K., & Parkin, S. (2024). Motivating employees to report phishing. European Symposium on Usable Security (EuroUSEC 2024).
Doing, A.-K., Bárbaro, E., van der Roest, F., van Gelder, P., Zhauniarovich, Y., & Parkin, S. (2024). Analysis of phishing reporting activity in a bank. Proceedings of EuroUSEC ’24.
Eijkelenboom, E. (2021). Cybersecurity disclosure in the banking industry: Evidence from the Netherlands. Journal of Accounting and Management Information Systems, 20(3), 321–340.
Ekeh, B., & Adigun, T. (2022). Secure coding techniques for resilient online banking platforms. *Software Security and Applications Journal, 8*(2), 71–88.
Ekong, E., & Bassey, S. (2023). Continuous authentication for preventing long-session account takeovers. *International Journal of Cyber Identity Management, 9*(1), 44–59.
Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks’ performance: the moderating role of corporate governance in the MENA region. Future Business Journal, 10, 115.

Fedele, A. (2024). Phishing attacks: An analysis of victims' characteristics. Psychiatry Research, 337, 115679.
Gowda, P., & Gowda, A. N. (2022). Zero Trust: A Paradigm Shift in Banking Cybersecurity. Journal of Economics & Management Research.
Jakovljević, N. (2022). Analysis of cyber threats as a risk factor in the banking sector. Bankarstvo, (3-4), 32-65. https://doi.org/10.5937/bankarstvo2204032j
Jimmy, F. (2024). Cybersecurity threats and vulnerabilities in online banking systems. International Journal of Scientific Research and Management, 12(10), 1631–1646.
Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation in emerging markets. Corporate Law & Governance Review, 7(1), 28–37.
Kareem, M., & Ndubuisi, L. (2022). Firmware vulnerability management in critical banking hardware. *African Journal of Cyber Infrastructure, 7*(1), 51–67.*
Makinde, O., & Osahon, P. (2023). Strengthening financial API security in Nigerian digital banking. *Journal of Fintech Systems Security, 6*(2), 103–120.*
Mensah, D. (2025). Governance-based cybersecurity models for sub-Saharan African banks. African Journal of Information Systems, 17(3), 210–232.
Metibemu, O. C. (2025). Financial risk management in digital-only banks: Addressing fraud and cybersecurity threats in a cashless economy. Asian Journal of Research in Computer Science, 18(3), 434-455.
Miya, N. F., & Joseph, N. (2025). Banking on resilience: 20 years of cybersecurity evolution. South African Journal of Information Management, 27(1), a2019.
Nwachukwu, J., & Adeleke, Y. (2023). Deception technology as a proactive defence in digital banking environments. *Cyber Defence Innovations Review, 12*(1), 60–75.
Ojo, F., & Salam, A. (2022). Sandboxing approaches for detecting advanced malware in banking networks. *International Journal of Malware Analysis, 4*(1), 26–42.
Onifade, T., & Musa, K. (2023). Automated policy enforcement and internal security compliance in banks. *Journal of Information Governance Studies, 10*(2), 88–105.
Peihani, M. (2022). Regulation of cyber risk in the banking system: A Canadian case study. Journal of Financial Regulation, 8(2), 139–161.
Rabiu, H., & Chima, R. (2024). Preparing for quantum-enabled cyberattacks through post-quantum cryptography. *Journal of Future Cybersecurity, 3*(1), 14–31.
Rahman, A., & Nasir, M. (2023). Artificial intelligence intrusion detection models in Asian banks. Journal of Banking Security & Technology, 8(4), 250–268.
Sulong, Z. (2025). Cybersecurity risk and bank risk-taking. International Journal of Finance & Banking Studies, 14(2), 77–94.
Ubah, J., & Solomon, D. (2021). Micro-segmented virtual infrastructures and banking data protection. *Journal of Cloud and Virtual Security, 5*(2), 99–115.
Yıldırım, Z. (2024). Securing digital transactions: The importance of cybersecurity in banking. Journal of Internet Banking & Commerce, 29(6).
Bamberger, G. (2020). RegTech in financial services: Technology solutions for compliance and risk management. *Journal of Financial Regulation*, 6(2), 245-261.
Bebchuk, L. A., & Spamann, H. (2010). Regulating bankers' pay. *Georgetown Law Journal*, 98, 247.
Berger, A. N., & Bouwens, J. (2009). Bank capital, risk, and performance. In *The Oxford Handbook of Banking*. Oxford University Press.
BCBS (Basel Committee on Banking Supervision). (2013). *Liquidity Coverage Ratio (LCR) and liquidity risk monitoring standards*. Bank for International Settlements.
Borio, C., & Disyatat, P. (2010). Liquidity and leverage. *Journal of Financial Intermediation*, 19(3), 335-357.
Boyd, J. H., & Graham, S. L. (1986). Risk, regulation, and bank holding company expansion into nonbanking. *Federal Reserve Bank of Minneapolis Quarterly Review*, 10(2), 2-17.
Flannery, M. J., & Kwan, S. H. (2005). Market discipline and bank subordinated debt: A review of the evidence. *Journal of Financial Services Research*, 27(2), 91-108.
FSB (Financial Stability Board). (2019). *FinTech and the financial system: A framework for considering its implications and supervisory responses*.
Goddard, J., Molyneux, P., & Wilson, J. O. (2009). *The economics of banking*. Wiley-Blackwell.
Gorton, G. (2012). misreading the crisis: The roots of the financial panic. *Cato Journal*, 32(3), 455-466.
Hirtle, B. (2018). The evolution of stress testing. *Federal Reserve Bank of New York Economic Policy Review*, 24(1), 1-16.
Jacobson, T., Lindé, J., & Roszbach, K. (2005). Credit risk versus capital requirements: A panel data analysis of Swedish banks. *Journal of Banking & Finance*, 29(12), 2955-2972.

Klein, N., & Weill, L. (2019). The determinants of non-performing loans: Evidence from an emerging market. *International Economics*, 159, 30-44.
Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics*, 93(2), 259-275.
Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, 18(4), 8-20.
Pathan, S. (2009). Strong boards, CEO power and bank risk-taking. *Journal of Banking & Finance*, 33(7), 1340-1350.