Evaluating Potential Dangers in the Banking Industry

CHETNA SIWACH
Galgotias University, Greater Noida

Abstract- The paper is called "Assessment of the Risks in the Banking Sector" and researches the topic of the multidimensional threats faced by banks in the modern complicated financial environment. With the support of the descriptive research design and the collection of quantitative data pursued among 60 banking professionals via structured questionnaires, the research unveils the most essential threats such as cybersecurity risks, credit risk, operational risk, and regulatory compliance issues. The results indicate cybersecurity as an most serious and urgent threat which is aggravated by the accelerated digital banking and dynamic technological threats. All the banks have done well in the operational risk management, but still there are gaps in technology infrastructure and trained staff. Another challenge to risk mitigation is presented by regulatory changes, especially in environmental, social and governance (ESG) compliance. The paper supports the idea of combined and adaptive risk management systems, human capital investment, and the improved cooperation of regulators as the means of enhancing the resilience of banking. These lessons are of great help to banking institutions, policy makers and academicians in their quest to ensure financial stability in a period of unparalleled complexity of risks.

Keywords- Banking industry, risk management, cybersecurity, credit risk, operational risk, regulatory compliance, digital banking, ESG compliance.

I. INTRODUCTION

3. Introduction

3.1 Study background

Banking industry forms a very significant pillar or part of the global financial system since it is the main intermediary through which flow of funds occurs between the savers and the borrowers. Banks play a role in the development of the economy since they provide vital services to the economy namely acceptance of deposits, credit provision, processing of payments and investments. The banking industry has experienced tremendous changes over the years, which have been as a result of globalization, technological advancement, deregulation, and the changing expectations of the consumers. The above developments have widened the horizons of banking business however, it has also brought in greater complexity and exposure to risks.

Traditionally, banks were dealing with familiar risks, like credit risk, which is connected to the potential default of a borrower, and market risk, caused by the changes in asset prices and interest rates. Yet, the past few decades could be characterized by a significant increase in both the variety and intricacy of threats that banks are faced with. Operation and cybersecurity risks have also been created by the emergence of digital banking and fintech innovations, which are concerned with technology failure, fraud, and cyber-attacks. At the same time, increased regulatory focus and changes in compliance demands have placed an extra burden and challenge on the governance arrangements of banks. This is a dynamic risk environment which requires thorough evaluation and dynamic approaches of risk management in order to ensure stability and viability of performance of the banking institutions.

3.2 Statement of the Problem

Nevertheless, banks have remained under considerable and transforming threats that have endangered the operational performance, financial performance, and the confidence of the people in the regulatory frameworks and risk management practices. In combination with the fast rate of technological transformations, the growing complexity of the cyber threat has increased these vulnerabilities beyond the potential coverage of the traditional risk management techniques. Also, banks face difficulties in operating within complicated and highly dynamic regulatory frameworks, such as fresh requirements linked to environmental, social, and governance (ESG) concerns.

Inability to properly identify, evaluate and manage these risks may lead to the significant loss of money, regulatory fines, reputational risks and even bankruptcy in worst scenarios. In addition, global financial markets have a strong interconnectedness meaning that risks that materialize in one institution may spread, thereby leading to the systemic crises. Thus, it is urgent to assess the situation with risks in all its breadth and depth, learn about the severity and prevalence of these threats, and analyze the quality of mitigation measures that are currently used. This is one of the issues that need to be addressed in order to create sustainable banking practice that will be able to adjust to the current changes and safeguard the interests of stakeholders.

3.3 Study Goals

The main aim of the study is the assessment of the threats that can be directed to the banking sphere, in particular, the evaluation of the essential risk types, their influence, and the effectiveness of current risk management. The particular aims include:

To detect and classify the main threats that banks are facing, both traditional risks (e.g., credit and market risk) and new threats (e.g., cybersecurity and regulatory compliance).

To determine the perceived severity and occurrence of the risks to the banking processes and financial stability.

To examine how effective the existing risk management models and regulatory compliance procedures are when it comes to limiting the identified threats.

To understand how technological developments, specifically digital banking and computer security procedures, determine banking risk exposure.

To come up with practical policy suggestions to banking institutions as well as regulators that would facilitate the improvement of risk identification, evaluation, and mitigation strategies.

With the help of these aims, the research will be aimed at adding to the sophisticated perception of the multifaceted risk environment of contemporary banking and the strategy that would facilitate sustainable resilience of the industry.

3.4 Research Questions

In order to focus the inquiry, the research paper seeks to answer the research questions below:

What are the key risks and possible threats which the banks have nowadays?

What are the effects of these risks to the operations and financial performance of the bank as well as the confidence of its stakeholders?

What is the ability of current regulatory policy and internal risk management structures to deal with these risks?

What are the issues facing the banks in the implementation of the risk management strategies particularly within the framework of technological innovations?

What are some practical steps that can be advised to enhance banking risk reduction and resilience of the institution?

The following questions are intended to put the research in its context and help to get a full scope of analysis of the issues that are relevant to banking risks.

3.5 Significance of the Study

The research is of great importance to different participants in the banking system. To banking practitioners and risk managers, the results provide a timely view on risk priorities and new threats, to help make better decision-making on risk governance and operational planning. The priority given to cybersecurity and regulatory compliance are the topical issues in the industry, and these are the areas where more beneficial effects can be achieved with the help of additional investments and dedicated strategic measures.

Policymakers and regulators can gain evidence-based knowledge on the sufficiency and issues of regulatory frameworks, particularly in respect to the ESG compliance and digital financial services, as an example of emerging areas. This can guide the making of flexible, neutral policies that both allow innovations and maintain financial stability and consumer protection.

On the academic side, the research is important as it has combined the classic and the new dimensions of risks in a new framework of the banking risk management literature. It points to some important gaps in knowledge and future research, especially with regard to how technology and regulation interact to create risk landscapes.

In social point of view, it is important to improve the knowledge and control of the banking risks to preserve the trust in the financial institutions which are the pillars of the economic development and stability. In solving the potential dangers before they occur, the banks can minimize the chances of having disruptive crises and protect the interests of the depositors, investors, and the entire economy.

3.6 Scope and Limitation

This research paper is framed in such a way that it takes a comprehensive view of risks in the banking sector, among the established and the new ones. The study relies upon survey research conducted among the banking practitioners and is enriched with secondary resources like trade publications and regulatory filings. The main types of risks that are considered are credit risk, operational risk, cybersecurity threats, market risk, liquidity risk, and regulatory compliance challenges, and special emphasis is made on the consequences of the adoption of digital banking and ESG concerns.

There are various drawbacks imposed on the generalizability and depth of the study. Purposive sampling method and the sample size though adequate to get the expert views, reduce the generalization of the findings to all the banking institutions and geographical locations. A cross-sectional design gives a point picture in time, so it can fail to represent changing risk dynamics. The researchers also give more priority to perception-based analysis instead of the quantitative models of risk measurement, which constrains the empirical accuracy of the impact analyses. Moreover, the regulatory peculiarities associated with jurisdiction and a very technical risk modeling method are beyond the parameters of the present research.

II. LITERATURE REVIEW

Banking sector has a significant role in overall financial system of the world since it is an intermediary that provides allocation of resources, management of liquidity and payment systems without which the economic growth would not be possible. In the past decades, the industry has been experiencing radical changes due to the forces of globalization, technological discoveries, and new regulatory environments (Jadwani, Parkhi, & Mitra, 2024). Such changes have increased the efficiency and accessibility, but have also created some complex vulnerabilities which have widened the magnitude and type of risks that banks have to handle. Banking risks Credit risk, focused on the potential of a borrower to default, is still the basis of risk management because it has a direct influence on asset quality and profitability (Jadwani et al., 2024). Additional attention is still required to be paid to market risk, associated with changes in interest rates, foreign exchange, and equity prices, and liquidity risk, which is linked to the capacity of the bank to clear its short-term liabilities (Patel, 2023). But in addition to these long-term threats, there has been increased focus on operational risk which includes losses due to internal failure, fraud and technology disruption. Banks have been facing new challenges due to the increasing use of digital banking services demonstrated in hacking, ransomware, and data breaches, which pose threats to financial and reputational stability (Kovacevic, Radenkovic, & Nikolic, 2024; Waliullah et al., 2025). The issue of cybersecurity has become one of the most important matters, as advanced cyber threat becomes more and more frequent and advanced, typically focusing on sensitive customer information and interfering with the functioning of the bank (Kshetri, Rahman, Sayeed, & Sultana, 2023). Moreover, compliance risk has been exacerbated in recent years as banks have to comply with a growing number of laws and standards, such as those related to anti-money laundering, know-your-customer procedures, and, to an increasing extent, environmental, social, and governance (ESG) (FDIC, 224; ABA, 224). ESG factors incorporated into risk management is an emerging aspect along which banks have to assess climate transition risks, as well as social liabilities, which can have a material impact on their credit

portfolios and reputational status (Nguyen et al., 2023; Palmieri et al., 2024). All these advancements highlight the dynamism of the complexity of risks in banking, necessitating a more profound and dynamic risk framework, which goes beyond the conventional financial risks to embrace the socio-technological risks on the rise.

The regulatory policy on banks has also simultaneously advanced to keep up with these varied risks and build up systemic resilience. Since the 2008 financial crisis, most of the reforms such as the Basel III accords have placed tough capital adequacy, leverage, and liquidity requirements on banks to make them resilient to shocks (Deloitte, 2024). In addition to capital regulation, supervisors have placed more attention on operational and cyber risk management, and they encourage banks to implement sophisticated cybersecurity measures and improve incident response readiness (FDIC, 2024). According to the American Bankers Association (ABA) (2024) and other trade organizations, it is also necessary to address innovation risk management, especially regarding the integration of artificial intelligence (AI), which has possible unintended consequences without proper control (Lyon & McCauley, 2024). Moreover, crypto-asset risks, and decentralized finance have become a focus of the regulators, expressing concern with the volatility, fraud, and regulatory arbitrage opportunities that threaten to erode the legacy banking business models (FDIC, 2024). Nevertheless, in spite of these regulatory developments, banks continue to struggle with the challenge of maintaining a fast technological change,Regular regulatory changes, and cross-jurisdictional compliance obligations (ABA, 2024; S&P Global Market Intelligence, 2025). Research highlights that the smaller institutions can be out-sized affected by the complexity of regulation, as well as resource pressures, which could make them more susceptible to non-compliance (S&P Global Market Intelligence, 2025). The empirical literature and industrial publications alike emphasise the vulnerability created by the reliance on technology and cyber vulnerability, and threaten of the systemic consequences in case of the critical events (Financial Times, 2025; Reuters, 2025). Also, the academic literature suggests closer cooperation between regulators and banks, more flexible regulatory frameworks that can promote innovation and ensure stability, the integration of scenario analysis and stress tests to predict the emerging risks (Bowman, 2025; Patel, 2023). In short, what the literature reveals about the banking environment is one where risk interdependencies are complex and regulatory environment attempts to provide a balance between prudence and dynamism to deal with a precedent set of both traditional and new threats.

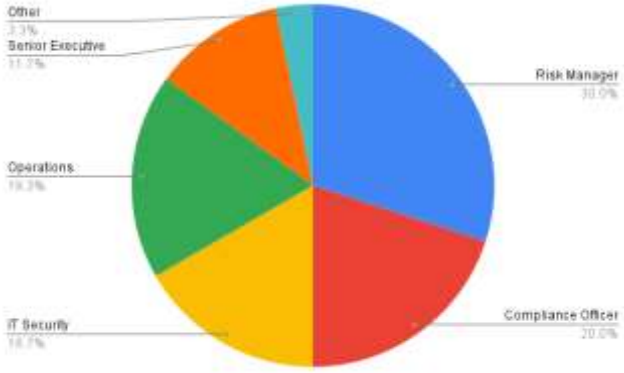
III. RESEARCH METHODOLOGY

In the given research, the descriptive research design will be utilized to conduct the systematic investigation of the potential threats the banking industry, as it allows the detailed observation and the description of the phenomena without controlling the variables. Specifically, the descriptive research is the most appropriate based on the research aim of determining the nature, frequency and the effect of the various banking risks and also determining the effectiveness of the risk management practices on practical basis. The main instrument of data collection was a structured questionnaire that was delivered electronically to a purposively sampled population of 60 banking professionals, comprising risk managers, compliance officers, IT security experts, operations managers and senior executives, who have the appropriate expertise and the first hand experience about the dynamic of risks within their organizations. Purposive sampling method was specifically adopted because the sampled respondents were required to possess enough experience and understanding which would enable them to give relevant data that is valuable and trustworthy in relation to the research questions. The construction of the questionnaire was guided by the thorough analysis of the available literature and industry recommendations, and it included demographic information, the recognition of the most important banking risks, the subjective assessment of the severity of risks, the usefulness of risk management measures, the level of awareness of regulatory and ESG compliance, and the difficulties in dealing with the emerging threats. It contained closed-ended questions as well as Likert-scale questions so as to enable me to perform quantitative analysis and to get consistency among the responses. The questionnaire was pilot tested on a small sample of banking professionals before the actual deployment to serve the purpose of giving clarity, relevance, and reliability, and further modifications were executed according to their response. The data was collected within a specified timeframe through online distribution, which was the most convenient way and considering the work schedules of the respondents. The collected data underwent through strict cleaning exercise so as to ascertain their completeness and accuracy and where necessary, incomplete or inconsistent responses were eliminated. Descriptive statistics in the form of frequency distribution, percentages, means, and standard deviations were used in quantitative data analysis to describe the demographics of the respondents and their main risk perceptions. Such inferential statistical methods as correlation analysis were used to test the relationships between the variables, such as risk awareness and management effectiveness. Data coding, entry and statistical processing were done using Microsoft Excel and the SPSS software package and graphical displays in terms of pie charts and bar graphs were produced to convey important results visually. Besides, Open-ended questions were embraced and their qualitative responses were coded and organized into themes to reveal common patterns and to addcontextual richness to quantitative findings. Ethics were considered in the entire research process whereby all the participants gave an informed consent, anonymity and confidentiality were strictly adhered to and the data was stored in password-protected files accessible by the researcher alone. No personal data was gathered, and the participation was voluntary, with the possibility of the respondents halting the participation at any moment, without incurring any cost. The design of the research methodology was to strike a balance between scientific rigor and practical limitation to provide dependable and relevant information about the dynamic risk environment in the banking sector and acknowledge the shortcoming concerning the sample size, purposive sampling and cross-sectional collection of data. On the whole, this methodology helps to conduct an in-depth and ethically responsible investigation of the many-sided threats that modern banks face, which will serve as the solid background to the further analysis of data and discussion.

IV. DATA ANALYSIS AND INTERPRETATION

Table 1: Distribution of Respondents by Job Role

	Frequency	Percentage (%)
Risk Manager	18	30
Compliance Officer	12	20
IT Security Specialist	10	16.7
Operations Manager	11	18.3
Senior Executive	7	11.7
Other	2	3.3
Total	**60**	**100**



Graph 1: Distribution of Respondents by Job Role (Pie Chart)

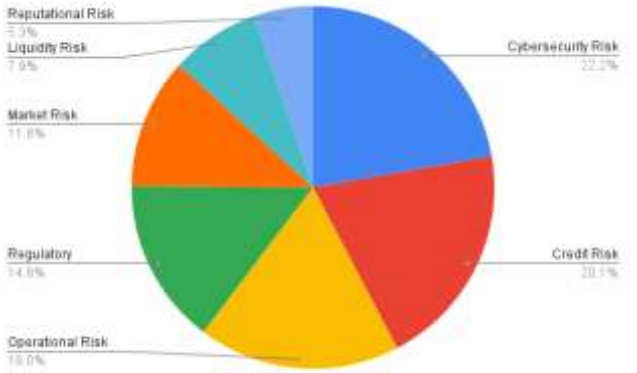
Interpretation:

The respondent profile indicates a wide-range of cross-section of risk and operational professionals in the banking industry. The greatest group is Risk Managers (30%), which underlines their central role in the process of risk identification and mitigation. More than one-third of respondents are Compliance Officers and IT Security Specialists, which evidences the relevance of regulatory compliance and information security in banking. The presence of the Operations Managers as well as the Senior Executive offers this feature of representation of the operational as well as strategic levels of leadership. This even spread offers a rich background of examining the risk perceptions among the major functional areas of the banks.

6.2 Identification of Key Banking Risks

Table 2: Key Banking Risks Identified by Respondents

	Frequency (Selected)	Percentage of Respondents (%)
Cybersecurity Risk	42	70
Credit Risk	38	63.3
Operational Risk	34	56.7
Regulatory Compliance	28	46.7
Market Risk	22	36.7
Liquidity Risk	15	25
Reputational Risk	10	16.7



Graph 2: Key Banking Risks Identified (Pie Chart)

Interpretation:

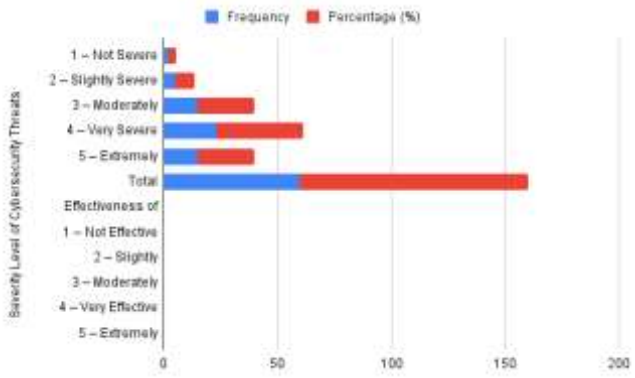
The most prominent issue is the cybersecurity risk, as 70 percent of the survey participants consider it one of the major threats. That highlights the growing importance of digital threats in a quickly developing technologic environment. The credit risk has been of crucial importance, as more than 60 percent of the respondents chose it, confirming once again its primary role in the financial stability. The operational risk has also been very well acknowledged which indicates the weakness in the internal processes and systems. Regulatory compliance remains a challenge as chosen by almost a half of the respondents pointing out to pressures due to growing regulatory requirements. Less popular, nevertheless, market, liquidity and reputational risks remain topical, and they demonstrate the versatility of banking risk profiles.

6.3 Assessment of Risk Impact and Management Effectiveness

Table 3: Perceived Severity of Cybersecurity Threats and Effectiveness of Risk Management

	Frequency	Percentage (%)
1 – Not Severe	2	3.3
2 – Slightly Severe	5	8.3
3 – Moderately Severe	15	25
4 – Very Severe	23	38.3
5 – Extremely Severe	15	25
Total	**60**	**100**

Effectiveness of Risk Management in Mitigating Operational Risks	**Frequency**	**Percentage (%)**
1 – Not Effective	3	5
2 – Slightly Effective	7	11.7
3 – Moderately Effective	21	35
4 – Very Effective	20	33.3
5 – Extremely Effective	9	15
Total	**60**	**100**



Graph 3: Severity of Cybersecurity Threats and Effectiveness of Risk Management (Bar Chart)

Interpretation:

The threat of cybersecurity is assessed by a large majority (63.3%) of respondents as very to extremely severe, which once again indicates the critical importance of this category of threats. A very few (11.6%) consider these threats as having minimal severity, which probably relates to differences in institutional exposure or the maturity of cybersecurity defenses. Concerning operational risk management, about half of the respondents (48.3 percent) feel that their frameworks are quite to highly effective, and they have confidence in existing controls. Nevertheless, 35 percent consider effectiveness average, which means that it could be enhanced, especially in terms of responding to the increasing complexity of technology-related risks. A small part of them (16.7%) raised the issue of the lack of effectiveness of risk management, which may indicate persistent problems with resources distribution, technology inclusion, or employee knowledge. Together, these findings highlight the urgent necessity of instituting a constant process of improvement with regards to cybersecurity preparedness and operational risk management frameworks in order to avoid the dynamic threats that are being faced by banks.

V. DISCUSSION

The results of the present study explain a picture of conflicting and dynamic risk environment in the banking sector in which the long-standing risks like credit risks and operational risks still persist and cause major problems, but new risks, specifically the cybersecurity threats, have taken a new dimension. Cybersecurity risk prevails among the respondents, which reinforces the idea of the dramatic change in the vulnerability landscape of the banking sector due to the digital shift and the embrace of technology. It also coincides with the existing literature in the area of increasing complexity and regularity of cyber-attacks, which poses a threat not only to the confidentiality and integrity of the financial information but also to the overall continuity of operations and the faith of the stakeholders (Kovacevic, Radenkovic, & Nikolic, 2024; Waliullah et al., 2025). Although it seems that banks have implemented moderately efficient operational risk management frameworks, large numbers of respondents reporting moderate or lower effectiveness levels point to the fact that there is still much work to do with regard to updating these frameworks to adapt to ever-changing technological threats. Furthermore, the problems of regulatory compliance, especially in ESG requirements and fast-changing legal requirements, indicate the growing complexity that banks experience when trying to align the strategic goal with the changing governance requirements (Nguyen et al., 2023; ABA, 2024). The ambivalent views regarding the sufficiency of the banks in terms of responding to the changes in regulations imply the absence of the even implementing abilities which may be explained by the lack of resources and organizational inertia. The fact that the human capital shortage and technological infrastructure constraints have been revealed as the major impediments also proves the necessity to make specific investments into the workforce and information technology modernization. The challenges are further complicated by the fact that more than a half of the respondents expect high possibility of significant risk-related events in the nearest future which on the one hand reflects the increased awareness but on the other hand demonstrates the feeling of vulnerability that can only be addressed by taking serious and effective risk reduction measures. The combination of this traditional and emerging risks, regulatory complexity and organizational limits confirm the necessity of integrated, advanced risk management strategies, which should include technological innovation, regulatory appropriateness, and human capital development. Banks should develop a risk culture, utilize advanced analytics and AI to achieve real-time monitoring, and actively collaborate with regulators and industry peers in order to predict and counter any systemic threats in an adequate manner. The results of the study can be added to the current body of knowledge in the sense that it empirically confirms the current risk concerns and shows where banking institutions and policymakers need to concentrate their efforts in order to enhance resilience. However, the constraints regarding the study sample size, the cross-sectional nature of the research, as well as the use of perception-based data indicate that these insights should be verified in future research where longitudinal and quantitative incident data would be used. On the whole, this paper can provide helpful insights to the banking stakeholders that need to find a way to operate in an environment with more complex risk environment and need to realize that only constant changes can survive in the era of fast technological and regulatory changes.

VI. CONCLUSION AND RECOMMENDATIONS

This paper has examined in detail the possible threats which the banking sector faces by incorporating the views of banking experts on both the classic risks facing the sector like credit risk and operational risk and the newer risks which are being brought mostly by the cyber security weaknesses and compliance issues. As the analysis shows, although the traditional threats still affect the financial stability of banks and the efficiency of their operations, the digitalization of the banking services at the rapid pace has multiplied the vulnerability to cyber-attacks and technology-related disruptions, demanding larger attention toward cybersecurity systems and dynamic risk management models. Although most institutions have made notable improvements in the management of operational risks, there still exist some big gaps, particularly in the ability to match the technological infrastructure and human capital resources with the ever changing risk environment. The increasingly prominent role of environmental, social, and governance (ESG) factors in regulatory frameworks also complicates the risk picture, who must now build flexible compliance frameworks that are able to properly incorporate sustainability considerations into their overall risk pictures. Particularly, the current survey reveals that a significant percentage of respondents expect high possibilities of occurring major risk events in the nearest future, which highlights the necessity to strengthen risk preparedness and response capacities. On the basis of these findings, it is urgent to recommend the banking institutions to invest, first of all, in the advanced cybersecurity technologies, such as AI-based threat detection and continuous monitoring systems, and promote a strong culture of risk awareness and responsibility at all levels of the organization. It is also of paramount importance to consider the skills gap, which can be accomplished by providing specific training and conducting collaboration with academic and professional organizations to make sure that staff members have the necessary knowledge and skills to deal with complex and emerging risks. Regulatory authorities also need to work in close association with the banks to assist in the creation of flexible, future-focused frameworks that are apt at facilitating innovation and maintaining systemic safety, offering certainty on emerging risk domains, including AI regulation and digital assets. Moreover, scenario planning and stress tests exercises should be routinely revised to take into consideration evolving threats, such as cyber-incidents and climate-related disruptions, to increase the resilience and contingency planning of banks. It is also possible to improve defenses against sophisticated threats by encouraging the banking industry to share more information and cooperate. Although this study contributes to knowledge of the complex risk environment, further research is required to create quantitative risk modelling, cross-jurisdictional comparative analysis, and behavioural aspects of risk management that can be utilised in evidence-based policy and strategic decision-making. In the end, an integrated, proactive attitude to risk identification, evaluation, and elimination will have to be adopted as the means of banking institutions retaining their financial stability and preserving the trust of stakeholders and being able to operate in the dynamic global financial environment with the required degree of success.

REFERENCES

American Bankers Association. (2024, December). *Top bank risks for 2025*. ABA Banking Journal. https://bankingjournal.aba.com

Bowman, M. (2025, June 7). Top Fed official promises overhaul of U.S. bank regulation. *Financial Times*. https://www.ft.com

Deloitte. (2024). Basel III endgame update: Implications and considerations. *The Wall Street Journal*. https://deloitte.wsj.com

Federal Deposit Insurance Corporation. (2024, May 22). *2024 risk review*. https://fdic.gov

Financial Times. (2025, May). Banks vulnerable due to tech dependence and cyber fragility. https://ft.com

Jadwani, B., Parkhi, S., & Mitra, P. K. (2024). Operational risk management in banks: A bibliometric analysis and opportunities for future research. *Journal of Risk and Financial Management, 17*(3), 95. https://doi.org/10.3390/jrfm17030095

Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024, November 28). Artificial intelligence and cybersecurity in banking sector: Opportunities and risks [Preprint]. *arXiv*. https://arxiv.org/abs/2412.04495

Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2023, November 24). cryptoRAN: A review on cryptojacking and ransomware attacks w.r.t. banking industry—threats, challenges, & problems [Preprint]. *arXiv*. https://arxiv.org/abs/2311.14783

Lima, L. G. d. (2023). Essentials of risk management in the banking sector. *Researchgate*. https://researchgate.net

Lyon, S., & McCauley, C. (2024). On unmanaged innovation risk from AI adoption in banks. *ABA Banking Journal*. https://bankingjournal.aba.com

Mirashk, H., Albadvi, A., Kargari, M., & Rastegar, M. A. (2024, October 30). News sentiment and liquidity risk forecasting: Insights from Iranian banks. *Risks, 12*(11), 171. https://doi.org/10.3390/risks12110171

Nguyen, Q., DiazRainey, I., Kuruppuarachchi, D., McCarten, M., & Tan, E. K. M. (2023). Climate transition risk in U.S. loan portfolios: Are all banks the same? *International Review of Financial Analysis, 85*, 102401. https://doi.org/10.1016/j.irfa.2022.102401

Palmieri, E., Ferilli, G. B., Altunbas, Y., Stefanelli, V., & Geretto, E. F. (2024). Business model and ESG pillars: The impacts on banking default risk. *International Review of Financial Analysis, 91*, 102978. https://doi.org/10.1016/j.irfa.2023.102978

Patel. (2023). Central bank interventions and liquidity risk during market stress. In *Exploring Financial Risk Management: A Qualitative Study*. https://researchgate.net

Reuters. (2025, April 23). Tariff turmoil casts pall over European banks' 2025 earnings power. https://reuters.com

S&P Global Market Intelligence. (2025, January 17). Banking risk: Key themes to watch in 2025. https://spglobal.com

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025, March 23). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review [Preprint]. *arXiv*. https://arxiv.org/abs/2503.22710