AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Business Management, Economics and Banking
ISSN (E): 2832-8078 Volume 47, April - 2026

IMPROVING CYBER RISK ASSESSMENT AND MANAGEMENT IN COMMERCIAL BANKS: THE EXPERIENCE OF UZBEKISTAN AND CONTEMPORARY APPROACHES

Karimov Shokhrukh Boydulla o‘g‘li
Independent Researcher, Tashkent State University of Economics Tashkent, Uzbekistan.
E-mail: shohruhkarimov51@gmail.com
ORCID: 0009-0009-5675-1181

ABSTRACT

This article examines the theoretical, institutional, and practical aspects of cyber risk assessment and management in commercial banks. The purpose of the study is to analyze the impact of digital transformation on cyber risks in banking, to examine modern approaches to cyber risk assessment and management, and to develop practical recommendations for the banking sector of Uzbekistan. The study applies a systemic approach, comparative analysis, legal and regulatory analysis, and institutional analysis. The findings show that the expansion of digital banking services, mobile applications, electronic payments, fintech integrations, and external digital infrastructures requires cyber risk to be treated not merely as a component of operational risk, but as an independent strategic risk affecting financial stability, operational continuity, and customer trust in commercial banks. The comparative analysis of international and national practices demonstrates that effective cyber risk management depends on corporate governance, risk appetite, information sharing, institutional coordination, and the improvement of digital literacy. Based on the results, the article proposes scientific and practical recommendations for improving cyber risk assessment and management in the commercial banks of Uzbekistan.

KEYWORDS

Cyber risk, cybersecurity, commercial banks, digital banking, operational risk, anti-fraud, operational resilience, continuous verification-based security, information sharing, institutional coordination.

Introduction

In recent years, digital transformation has fundamentally reshaped the structure of financial services in commercial banks. The expansion of mobile banking, internet banking, remote identification, electronic wallets, QR payments, automated scoring platforms, fintech integrations, and external digital infrastructures has enhanced the speed, convenience, and accessibility of banking services. At the same time, however, this process has broadened the scope of cyber threats in banking operations and generated new risks and vulnerabilities.

Under the traditional approach, banking risks have generally been assessed within the framework of credit, market, liquidity, and operational risks. Yet, as the share of digital services has continued to

increase, the significance of the cyber component within operational risk has grown sharply. As a result, cyber risk is no longer merely a narrow technical issue confined to information security; rather, it has emerged as an independent strategic risk that directly affects a bank's financial stability, operational continuity, customer trust, and reputational standing.

International practice also confirms the growing relevance of this issue. In its principles for operational resilience, the Basel Committee treats cyber incidents as events associated with operational risk and emphasizes that banks must be prepared to ensure the continuity of critical operations. The International Monetary Fund, in turn, notes that severe cyber incidents may undermine confidence in financial institutions, disrupt critical services, and adversely affect the stability of the financial system. Therefore, cyber risk assessment and management are of crucial importance not only from the perspective of an individual bank, but also from that of the financial system as a whole.

In Uzbekistan, the significance of this issue is even greater. The digitalization of the banking system, the expansion of financial inclusion, the wider provision of remote banking services, and the introduction of modern payment technologies have become key priorities of the state's economic policy. Consequently, this has created an objective need to strengthen cybersecurity in commercial banks and to improve mechanisms for the early identification, assessment, and management of cyber risks.

In recent years, the national legal framework in the field of cybersecurity has also been significantly strengthened. In particular, the Law "On Cybersecurity" established a legal basis for the classification of critical information infrastructure facilities, the determination of mandatory requirements for such facilities, the conduct of monitoring, and the formation of a system for managing cybersecurity incidents.

In addition, Resolution No. PQ-153, adopted on April 30, 2025, set out practical measures aimed at strengthening efforts to combat cybercrime in the banking and financial sector and reinforced the protection of customer interests and financial security as a priority objective. The Resolution also provides for procedures for recovering material damages caused by non-compliance with information and cybersecurity requirements, the integration of transactional data into the Central Bank's unified platform, and the further development of a centralized anti-fraud system.

At the same time, a review of the academic literature indicates that, although cyber risk has been addressed from the perspectives of banking risk theory, digital financial services, operational risk, and institutional governance, studies assessing cyber risks in Uzbekistan's commercial banks through a comprehensive economic and institutional approach remain insufficient. In particular, there is still a need to examine cyber risk as an integrated system linked to corporate governance, operational resilience, information sharing, risk appetite, and customer confidence.

The purpose of this article is to analyze the theoretical, institutional, and practical aspects of cyber risk assessment and management in commercial banks under conditions of digital transformation, to comparatively evaluate international and national approaches, and to develop scientific and practical recommendations for banking practice in Uzbekistan. In line with this objective, the article examines the economic nature of cyber risks, the mechanisms through which they affect banking operations, the features of the national legal and institutional environment, and the main directions for improving cyber risk management.

Literature Review

In the international academic literature, banking risks have traditionally been examined within the framework of credit, market, liquidity, and operational risks. However, under conditions of rapid development in digital banking, mobile financial services, fintech integrations, and cloud-based infrastructures, cyber risk has moved beyond being merely a component of operational risk and is increasingly being recognized as an independent strategic threat with a direct impact on the activities of commercial banks. This trend is particularly evident in countries where payment systems, remote service channels, and data exchange processes are highly digitalized.

The French economist J. Bessis considers risk to be an important economic factor affecting bank performance[1]. In his view, risk is associated with potential losses that a bank may incur and can be assessed through both quantitative and relative indicators. This approach makes it possible to evaluate cyber risk not merely as a technical failure or unauthorized access to information systems, but as an economic risk that may lead to financial losses, service disruptions, inefficient use of resources, and declining customer confidence.

Among local researchers, J.E. Rabbimov analyzes the theoretical foundations of operational risk assessment in commercial banks and characterizes operational risk as the risk of financial loss arising from internal processes, human factors, system failures, and external events. According to the author, fraud, human error, technological disruptions, and legal or regulatory risks may adversely affect a bank's financial stability and business reputation[2]. In this regard, his approach provides an important theoretical basis for interpreting cyber risk as one of the most dynamic forms of operational risk associated with a bank's digital infrastructure, information systems, and remote service channels. He also identifies the three lines of defense model, the Basel II and Basel III approaches, and enterprise-wide risk management principles as important methodological tools for the assessment and management of operational risk.

Studies devoted to the development of digital technologies and financial services emphasize that the expansion of electronic payments, fintech services, and internet-based financial transactions is creating new economic relationships. While such studies highlight the positive effects of digitalization in terms of speed, convenience, and broader service coverage, they also point to its negative aspects, including the growing risk of cybercrime, the lag of legal frameworks behind technological development, and the increasing complexity of risk management processes. Thus, digitalization and cyber risk should be viewed not as contradictory phenomena, but as interrelated processes[3].

G.Q. Zakirova's research offers a detailed analysis of the role of digital technologies in the development of financial services. Her study examines the distinctive features of digital financial services as compared to traditional ones, the institutional cooperation between fintech companies and commercial banks, as well as the trends in the development of remote service delivery. The author emphasizes that digital services enhance speed, convenience, and efficiency for customers. At the same time, she notes that these digital channels may also generate new technological and information-related

[1] Bessis J. *Risk Management in Banking*. 4th ed. Wiley, 2015; Basel Committee on Banking Supervision. *Principles for Operational Resilience*. Basel: BIS, 2021.
[2] Rabbimov Jahongir Eshboyevich. Theoretical Foundations of Operational Risk Assessment in Commercial Banks // Journal of Finance and Banking. 2023.
[3] Muminova Masuda Bakhtiyorovna, Karimov Sardor Keldiyor ugli. Digital Economy and its Connection with Financial Technologies // Central Asian Academic Journal of Scientific Research. 2022. Vol. 2, Issue 5.

risks for banks. From this perspective, her research substantiates the need to treat cyber risk as an independent subject of study in the context of expanding digital banking services[4].

Approaches developed by international organizations provide a broader understanding of the significance of cyber risk. The Basel Committee's principles on operational resilience stress that banks must be prepared to ensure the continuity of critical operations and that cyber incidents should be regarded as serious events associated with operational risk. The U.S. National Institute of Standards and Technology, through its cybersecurity framework, recommends managing cyber risk through interconnected processes such as governance, risk identification, protection, detection of threats, response, and recovery. Similarly, the zero trust approach demonstrates that information security should not be limited to the protection of an external perimeter, but should instead require continuous verification of each user, device, and session.

Research by the International Monetary Fund treats cyber threats as an increasingly significant risk affecting not only individual financial institutions but also the stability of the financial system as a whole. These materials emphasize that severe cyber incidents may lead to declining confidence in financial institutions, disruption of critical financial services, and the amplification of negative effects through inter-institutional interconnectedness. As a result, such events may pose a serious threat to macroeconomic and financial stability. World Bank materials likewise interpret cybersecurity in the financial sector as a complex process linked to regulatory coordination, information sharing, and supervisory mechanisms.

In Uzbekistan, the legal and institutional foundations for cybersecurity have also been gradually strengthening. The Law "On Cybersecurity" established the legal basis for critical information infrastructure facilities, mandatory requirements, monitoring, and the management of cybersecurity incidents. In addition, Resolution No. PQ-153, aimed at strengthening efforts to combat cybercrime in the banking and financial sector, defined practical tasks such as protecting customer interests and financial security, integrating transactional data into a unified platform, and developing a centralized anti-fraud system. Reports of the Central Bank and materials related to the activities of CERT-CBU also confirm the growing institutional importance of cybersecurity in the information infrastructure of payment systems and commercial banks.

Thus, the review of the literature demonstrates that in contemporary academic approaches, cyber risk is no longer interpreted merely as a technical or information security issue, but rather as a complex economic risk closely linked to financial performance, operational resilience, institutional governance, and customer trust in banking activities. At the same time, the local literature still lacks sufficiently comprehensive studies that examine cyber risk from the perspective of a bank's overall risk profile, corporate governance, operational resilience, and intersectoral coordination. The scientific significance of this article lies precisely in addressing this gap.

Research Methodology

The primary objective of this study is to analyze the nature of cyber risks in commercial banks under conditions of digital transformation, the mechanisms through which such risks affect banking operations, and the specific features of their management; to comparatively assess international and

[4] Zakirova Gulnoza Kudratovna. The role and importance of digital technologies in the development of financial services // Journal of New Century Innovations. 2023. Vol. 23, Issue 3.

national approaches; and to develop scientific and practical recommendations for banking practice in Uzbekistan.

To achieve this objective, the study addresses the following tasks. First, it identifies the economic essence of cyber risks in commercial banking and determines the ways in which they differ from traditional operational risks. Second, it assesses the impact of cyber threats on banks' risk profiles in the context of the expansion of digital banking services, fintech integrations, and remote service channels. Third, it analyzes approaches to cyber risk assessment and management proposed by international organizations and standard-setting institutions. Fourth, it examines the specific features of the legal and regulatory framework as well as the institutional environment of cybersecurity in Uzbekistan's banking and financial sector. Fifth, it develops practical recommendations aimed at improving cyber risk assessment and management in commercial banks.

The scientific novelty of the study lies in the fact that cyber risk is substantiated not merely as a technical issue related to information security in commercial banking, but as an independent strategic risk affecting financial stability, operational continuity, corporate governance, and customer confidence. In addition, the study provides a comprehensive analysis of the economic and institutional nature of cyber risks in the context of the expansion of digital banking services.

Another scientific contribution of the article is that it offers a comparative assessment of international and national approaches and identifies the key directions that are essential for improving the cyber risk management system in the practice of commercial banks in Uzbekistan. In particular, the study provides a scholarly justification for the need to integrate cyber risks into corporate governance systems, develop risk appetite indicators, strengthen information-sharing mechanisms, improve digital and financial literacy, and adopt a comprehensive approach to the assessment of cyber incidents.

Thus, the theoretical significance of this research is reflected in clarifying the role and nature of cyber risks within the overall banking risk system, while its practical significance lies in the development of recommendations aimed at strengthening cybersecurity and improving cyber risk management mechanisms in commercial banks.

Analysis and Discussion of Results

The analysis conducted in this study demonstrates that the significance of cyber risk in the activities of commercial banks increases sharply as digital transformation deepens. Mobile banking, internet banking, electronic payments, QR infrastructure, remote identification, and fintech integrations enhance the speed and accessibility of banking services, but at the same time they create new entry points for cyber threats. As a result, cyber risk can no longer be regarded as a narrow component of traditional operational risk; rather, it has emerged as an independent strategic threat directly affecting a bank's financial stability, operational continuity, customer trust, and competitiveness.

The findings also indicate that the impact of cyber incidents on banking operations is not limited to technical failures or unauthorized access to information systems. Their consequences extend to financial losses, service disruptions, erosion of customer confidence, reputational damage, legal liability, and the weakening of interconnections among market participants. From this perspective, cyber risk should not be treated solely as an information protection issue, but rather as a complex risk that influences the economic outcomes of banking activity.

The study further shows that the relationship between the development of digital financial services and cybersecurity is not one-dimensional. Although digital services improve the efficiency of banking

operations, they simultaneously intensify technological and informational vulnerabilities. The expansion of remote service channels, mobile applications, external digital integrations, and payment platforms generates new technological and institutional risks for banks. Therefore, digital transformation and cybersecurity should not be viewed as opposing phenomena, but rather as interrelated and mutually influential processes.

The analysis also revealed certain differences between international and national approaches. In international practice, cybersecurity is considered in close connection with corporate governance, operational resilience, risk appetite, information sharing, and accountability systems. In the national context, although legal and institutional foundations have been established in these areas, their practical implementation across all commercial banks remains uneven and incomplete. This suggests that the existence of a regulatory framework alone is insufficient; such provisions must also be effectively implemented within banks and deeply integrated into management practice.

The analysis of Uzbekistan's experience confirms that significant practical steps have been taken toward the institutionalization of cybersecurity. In particular, the Law "On Cybersecurity" established the legal foundations for critical information infrastructure, monitoring, and the management of cybersecurity incidents. Resolution No. PQ-153 brought anti-cybercrime efforts in the banking and financial sector to a more practical stage by reinforcing such priorities as the protection of customer interests and financial security, the integration of transactional data into the Central Bank's unified platform, and the development of a centralized anti-fraud system. In addition, materials related to the activities of the Central Bank and CERT-CBU indicate the growing institutional importance of cybersecurity within the information infrastructure of payment systems and commercial banks.

The results of the study also substantiate the particular importance of an institutional approach to cyber risk assessment. Cybersecurity is not merely a function of protecting a bank's internal information systems; rather, it represents an institutional process based on the interdependence among the Central Bank, payment system operators, payment organizations, fintech entities, and other market participants. In this regard, strengthening information sharing, coordination, accountability, and responsibility mechanisms is an essential condition for ensuring the stability of the banking sector.

The study further demonstrates that technical protection tools alone are insufficient for the effective management of cyber risks in banks. Equally important are the internal control environment, a culture of risk awareness, staff competence, the digital and financial literacy of customers, incident response systems, reserve infrastructure, and mechanisms for information exchange. Thus, only a comprehensive and multi-layered approach to cybersecurity can ensure digital resilience in commercial banks.

Overall, the analysis and discussion of results show that, in the context of the digital economy, cyber risk has evolved into a category of risk that is not only technical, but also economic, institutional, and strategic in nature for commercial banks. Based on a comparative examination of domestic and international sources, it can be concluded that effective cybersecurity management is an essential prerequisite for maintaining a bank's financial stability, the reliability of digital services, and an environment of trust among market participants.

Conclusion and Recommendations

The findings of this study demonstrate that, under conditions of digital transformation, cyber risk in the activities of commercial banks has evolved beyond being merely a component of operational risk

and has increasingly become an independent category of strategic risk. The digitalization of banking services, the expansion of remote service channels, mobile banking, electronic payments, fintech integrations, and growing data exchange have improved the efficiency of banking operations. At the same time, however, these processes have widened the scope of cyber threats and created new economic, organizational, and institutional risks for banks.

The study confirms that it is insufficient to treat cyber risk solely as a technical issue or an information protection problem. Cyber risks manifest themselves through financial losses, service disruptions, declining customer confidence, reputational damage, legal liability, and negative spillover effects arising from the interconnectedness of participants in the financial system. Therefore, cyber risk should be analyzed as an integral part of the overall risk profile of commercial banks, particularly from the perspective of financial stability, operational continuity, and corporate governance.

The literature review, methodological framework, and empirical findings confirm the economic and institutional nature of cyber risk. In particular, a comparative examination of international and national sources shows that cybersecurity is a complex process closely linked to corporate governance, operational resilience, information sharing, risk appetite, and customer trust. The analysis also indicates that, although Uzbekistan has established legal and institutional foundations for ensuring cybersecurity, the issue of implementing them uniformly and effectively across all commercial banks remains highly relevant.

On this basis, the following recommendations are proposed.

First, cyber risks in commercial banks should be institutionalized as a separate category of strategic risk. To this end, cyber risk should be assessed not merely as part of operational risk in general terms, but as an independent area directly affecting financial stability and the continuity of digital services.

Second, cyber risk management should be deeply integrated into the corporate governance system. Establishing a clear allocation of responsibilities and accountability among the supervisory board, executive management, risk management, information security, and internal audit divisions would improve the effectiveness of cybersecurity governance in banks.

Third, it is advisable to develop a cyber risk appetite framework and a system of key indicators. Banks should introduce indicators that make it possible to assess the probability of cyber incidents, their scope of impact, service outage duration, the scale of financial losses, and their effect on customer trust.

Fourth, international approaches to cybersecurity should be adapted to national banking practice. In particular, commercial banks should gradually introduce practices related to operational resilience, continuous monitoring, rapid incident response, recovery planning, and the establishment of acceptable disruption thresholds for critical operations.

Fifth, information sharing among commercial banks, the Central Bank, payment system operators, and fintech entities should be strengthened. A system for the prompt exchange of information on cyber incidents, fraud schemes, and emerging threats would improve the early detection and containment of cyber risks.

Sixth, digital and financial literacy among employees and customers should be enhanced. Since a significant share of cybercrime is linked to the human factor, it is important to establish ongoing preventive awareness measures, training programs, and warning mechanisms.

Seventh, qualitative and quantitative methods of cyber risk assessment should be integrated. In this regard, it is advisable to develop a comprehensive assessment model that takes into account the

probability of cyber incidents, their economic consequences, reputational effects, impact on customer confidence, and the risk of cross-sector contagion.

Eighth, reserve infrastructure and recovery mechanisms should be strengthened. Improving data storage and recovery systems, backup centers, business continuity plans, and rapid response algorithms is essential for ensuring the digital resilience of banks.

Overall, the findings of the study show that improving cyber risk assessment and management in commercial banks is a crucial condition for ensuring the stability of the banking system in the digital economy. Measures aimed at strengthening cybersecurity contribute to the enhancement of banks' financial stability, customer confidence, competitiveness, and the effectiveness of digital services. From this perspective, improving the cyber risk management system should be regarded not merely as a technical necessity, but as one of the strategic priorities of banking activity.

REFERENCES

1. Law of the Republic of Uzbekistan. (2019). On Banks and Banking Activity (No. ZRU-580, November 5, 2019). Lex.uz.
2. President of the Republic of Uzbekistan. (2020). On the Strategy for Reforming the Banking System of the Republic of Uzbekistan for 2020–2025 (Decree No. UP-5992, May 12, 2020). Lex.uz.
3. Law of the Republic of Uzbekistan. (2022). On Cybersecurity (No. ZRU-764, April 15, 2022). Lex.uz.
4. President of the Republic of Uzbekistan. (2025). On Measures Aimed at Further Strengthening the Fight Against Crimes Committed through Information Technologies (Resolution No. PQ-153, April 30, 2025). Lex.uz.
5. Abdullaeva, Sh. Z., & Azizov, U. O'. (2019). Bank risklari [Bank Risks]. Tashkent: Iqtisod-Moliya.
6. Bessis, J. (2015). Risk Management in Banking (4th ed.). Wiley.
7. Rabbimov, J. E. (2023). Tijorat banklarida operatsion risklarni baholashning nazariy asoslari [Theoretical foundations of operational risk assessment in commercial banks]. Moliya va Bank ishi Jurnali, (2), 1–8.
8. Zakirova, G. Q. (2023). Moliyaviy xizmatlarni rivojlantirishda raqamli texnologiyalarning o'rni va ahamiyati [The role and importance of digital technologies in the development of financial services]. Journal of New Century Innovations, 23(3), 69–74.
9. Muminova, M. B., & Karimov, S. K. O'. (2022). Raqamli iqtisodiyot va uning moliyaviy texnologiyalar bilan aloqasi [The digital economy and its relationship with financial technologies]. Central Asian Academic Journal of Scientific Research, 2(5), 234–236.
10. Central Bank of the Republic of Uzbekistan. (2025). About the Cybersecurity Center "CERT-CBU". Official information. Retrieved April 7, 2026, from the Central Bank of Uzbekistan website.