WEP Warwick Evans Publishing

International Journal of Global Economics and Management

ISSN: 3005-9690 (Print), ISSN: 3005-8090 (Online) | Volume 10, Number 4, Year 2026
DOI: https://doi.org/10.62051/ijgem.v10n4.02
Journal homepage: https://ijgem.org

Research on Operational Risk Management of Commercial Banks Amid the Development of Financial Technology

Chen Chen

School of Business, Macau University of Science and Technology, Avenida Wai Long, Taipa, Macau, China

ABSTRACT

The deepening of digital transformation and the deep integration of financial technology and commercial bank management have not only optimized business processes and improved service quality and efficiency, but also presented new characteristics of increased concealment and diversified causes of operational risks. Traditional operational risk management frameworks are facing adaptability challenges. Based on the regulatory rules of the National Administration of Financial Regulation (NAFR), authoritative industry statistical data, and the practical application of financial technology in state-owned large banks, this article systematically analyzes the dual impact of financial technology on bank operational risk, sorts out the existing weaknesses and underlying causes of risk management, and proposes adaptive optimization solutions. Practice has shown that although financial technology effectively reduces traditional risks related to manual operations, it also gives rise to new risks such as data security and algorithm model bias. In addition, the insufficient supply of interdisciplinary talents and the lagging iteration of internal control systems continue to constrain the effectiveness of risk control. This study can provide practical references for commercial banks to improve their operational risk management system and strengthen their risk prevention and control capabilities through the use of financial technology, and help banks achieve stable operations in digital transformation.

KEYWORDS

FinTech; Commercial banks; Operational risk management; Intelligent risk control; Talent Reserves; Data Security

1. INTRODUCTION

The widespread application of digital technology promotes the in-depth integration of technologies such as big data, artificial intelligence, cloud computing, and privacy computing into core business scenarios such as commercial bank credit approval, payment and settlement, wealth management, and retail finance. The traditional offline business model is gradually being transformed towards online, intelligent, and intensive directions. In 2024, the total investment in financial technology by the six major state-owned commercial banks reached 125.459 billion yuan. The technology investment of Industrial and Commercial Bank of China, Agricultural Bank of China, and Construction Bank were 28.518 billion yuan, 24.970 billion yuan, and 24.433 billion yuan, respectively. The overall technology talent team in the industry continues to expand, and the layout of financial technology has become a key support for commercial banks to build differentiated competitive advantages and improve operational efficiency. In the process of digital transformation, new types of risk events such as network security risks, algorithm model defects, sensitive customer information leaks, and intelligent system operation failures continue to emerge. The original operational risk management model relying on manual verification and offline control is difficult to

adapt to the new risk forms [1]. The National Administration of Financial Regulation (NAFR) has clarified that operational risks include internal process loopholes, personnel operational errors, information system defects, and various losses caused by external emergencies. The popularization of financial technology has further extended the risk trigger points and risk propagation channels, significantly improving the concealment and diffusion speed of risks. This paper takes the operational risk control of commercial banks in the financial technology application context as the research object. It first defines the core concepts, then systematically analyzes the dual mechanism of technological application on operational risks, summarizes the prominent problems and root causes in the industry's risk management practice, and construct corresponding optimization strategies based on regulatory requirements and mature industry experience. It provides practical reference ideas for commercial banks to improve operational risk control mechanisms, balance innovative development and risk control, and achieve sustainable and stable operation amid the digital transformation of financial technology.

2. DEFINITION OF RELATED CONCEPTS

Financial technology is not simply a technical concept, but a product of the deep integration of digital technology and financial services. Technologies such as big data, artificial intelligence, cloud computing, and privacy computing are implemented throughout the entire process of financial services. Through technology-driven financial innovation, they promote the iteration of financial products, optimization of business processes, and upgrading of risk prevention and control capabilities. This is also the core definition of financial technology by the Financial Stability Board (FSB) and the People's Bank of China (PBOC). Its essence still belongs to the financial category, and its core value lies in using technological means to break through the efficiency bottleneck of traditional financial services, resolve risk control pain points, and enable financial services to serve various stakeholders accurately and conveniently, adapting to the diversified financial needs of the real economy [2].

The operational risk of commercial banks has a clear regulatory definition. In the "Management Measures for Operational Risk of Banking and Insurance Institutions" issued by the National Administration of Financial Regulation (NAFR) in 2023, it is defined as the risk of loss caused by internal process loopholes, employee operational errors, deficiencies in information technology systems, or external event impacts. This type of risk includes legal risk, but is not included in the scope of strategic risk and reputation risk. In industry practice, the manifestations of operational risk are both traditional and new, including long-standing traditional forms such as human operation errors and business process design defects, as well as new forms that have emerged with the development of the industry such as network attacks, sensitive customer information leakage, and third-party cooperation breaches [3].

After the comprehensive penetration of financial technology into the operation and management of commercial banks, the core orientation of operational risk management has also undergone a transformation. The current operational risk management has long departed from a simple risk avoidance mindset, relying on the technological advantages of financial technology to achieve precise identification, real-time monitoring, and effective prevention and control of various operational risks. The core of commercial banks' operations lies in stability, and business innovation empowered by financial technology cannot be separated from the bottom line of risk control. Only by embedding intelligent risk control tools into the entire business process, can innovative development and risk prevention achieve in-depth synergy, and truly unleash the value of financial technology, achieving a two-way balance between business development and risk control.

3. THE DUAL IMPACT OF FINANCIAL TECHNOLOGY ON OPERATIONAL RISK OF COMMERCIAL BANKS

The deep integration of financial technology into the business operations of commercial banks presents a distinct dual impact on operational risk. It not only streamlines traditional risk control and improves efficiency, but also gives rise to new risk challenges accompanied by digital technology. The two impacts are intertwined and become an important issue that cannot be ignored in the stable operation of banks [4]. Empowered by technology, intelligent means have gradually replaced a large number of manual operation processes, greatly reducing the probability of traditional operational risks such as human errors and process omissions. According to the Industry Development Report of the China Banking Association, commercial banks that have implemented AI-based risk control systems have seen an average decrease of 31% in non-performing loan rates, fraudulent transaction recognition rates increased to 96%, and an 8-fold increase in response speed to risk control decisions compared to traditional manual models. The "Smart Risk Control 3.0" system developed by Industrial and Commercial Bank of China can achieve real-time capture and analysis of transaction risks in all scenarios. Risk events can trigger precise warnings within 15 minutes of occurrence, which is 40 times more efficient than traditional manual monitoring modes. It effectively avoids operational risks in counter bookkeeping, offline verification, and other processes.

However, the deep application of financial technology has also given rise to new operational risks, which have stronger concealment and faster transmission speed, and are much more difficult to control than traditional risk forms. According to the statistics of fines in the field of financial regulation in 2025, more than 50 banks have been punished for violating financial technology management regulations, with small and medium-sized banks accounting for nearly 80%. Institutions such as Wuhai Bank have also been subject to "dual punishment" for failing to report cybersecurity incidents in a timely manner. Multiple rounds of regulatory notifications have also pointed out that financial apps under multiple banks have violated regulations by collecting sensitive personal information and excessively requesting permissions, highlighting vulnerabilities in data security management. At the same time, problems such as algorithm bias in AI models, sudden failures in intelligent systems, and outsourcing risks in third-party technology cooperation have also emerged one after another. The risk of data leakage in the banking industry has been ranked first in various industries for many years [6], and specialized attacks on financial data by illegal cyber industrial chain are becoming increasingly frequent. These new problems overlap with each other, posing unprecedented new challenges to the risk control system of commercial banks.

4. THE CURRENT SITUATION AND PROBLEMS OF OPERATIONAL RISK MANAGEMENT IN COMMERCIAL BANKS AMID THE DEVELOPMENT OF FINANCIAL TECHNOLOGY

In the context of digital transformation in the industry, domestic commercial banks generally attempt to optimize their operational risk management models through financial technology, continuously increasing technological investment and introducing intelligent risk control tools. However, from the perspective of industry practice and regulatory disclosure information, there are still significant shortcomings in the existing risk control system, and the effectiveness of operational risk control has not met expectations. In 2024, the financial technology investment of the six major state-owned commercial banks increased by 2.15% compared to the previous year, and the proportion of technology-related personnel in top institutions generally exceeded 5%. Among them, the proportion of technology-related personnel in Industrial and Commercial Bank of China reached 8.6%. Most banks have established intelligent risk monitoring and early warning frameworks, but small and medium-sized banks are significantly lagging behind in the depth of technology application, and the overall development level is uneven.

The prominent issues in current industry operational risk management are mainly reflected in four dimensions. Firstly, there is a severe shortage of interdisciplinary talents. Relevant statistics show that there will be an average annual shortage of nearly 200,000 domestic fintech talents in the next five years, with a total shortage exceeding one million. The proportion of professionals within banks who possess both technical capabilities and risk control experience is less than 3%. The talent gap directly restricts the deep integration of technology and risk control business [6]. Secondly, there are design and application flaws in the intelligent risk control models. Some institutional models have failed due to issues such as single data samples and regional feature deviations. In 2024, Qilu Bank and Quanzhou Bank were both fined large amounts due to incomplete risk control mechanisms. Model risk has become an important source of operational risk [7]. Thirdly, there are obvious loopholes in data security governance. Digital business brings massive data accumulation, and some banks have not implemented strict classification and grading management requirements. In 2024, more than 80 banking institutions were reported by regulators for information leakage and illegal collection of user data. The privacy leakage incident caused by information outsourcing of WeBank is a typical cautionary case. Finally, the construction of internal control system lags behind technological development. The original internal control rules are mostly formulated around offline business, lacking effective coverage of new scenarios such as online business, intelligent system operation and maintenance, and third-party cooperation. The process design is rigid and cumbersome, and cannot adapt to the operational rhythm of digital business.

5. ANALYSIS OF THE CAUSES OF OPERATIONAL RISK MANAGEMENT ISSUES IN COMMERCIAL BANKS AMID THE DEVELOPMENT OF FINANCIAL TECHNOLOGY

Based on the actual operational situation of the industry and current regulatory requirements, the various problems that arise in the operational risk management of commercial banks are not caused by a single factor, but rather the result of the combined effect of multiple factors such as the implementation of technology applications, talent training systems, internal control mechanism construction, and coordination between supervision and the industry. This phenomenon is particularly evident in small and medium-sized banks that have a slow pace of digital transformation. Some institutions place excessive emphasis on the investment volume of financial technology, blindly introducing intelligent risk control systems and digital business platforms without fully matching their own risk control needs, weakening the depth of integration between technology and risk management scenarios, and lacking regular verification of the compliance, stability, and interpretability of AI models. Model deviations, system vulnerabilities and other issues directly lead to new operational risks, and accordingly have become major reasons for regulatory penalties in recent years. The existing talent cultivation of commercial banks is mainly based on basic operational skills, and has not built a comprehensive talent cultivation system covering technology, business, and risk control. Superimposed with the competitive pressure of the Internet industry, the problem of core scientific and technological personnel loss continues to intensify. According to data from the Institute of Financial Technology at Tsinghua University, the shortage of core talents in financial technology in the domestic banking industry has exceeded 350,000, with less than 3% of professionals possessing both technical skills and risk control experience. The talent gap directly restricts the actual effectiveness of technology-enabled risk control. The current internal control system still focuses on offline business as the core, and there are gaps in the control rules for new scenarios such as online business, intelligent system operation and maintenance, and third-party technology cooperation. The internal control supervision mainly focuses on ex-post verification and rectification, and the mechanism construction of pre-warning and in-process blocking is obviously insufficient. At the same time, the iteration speed of financial technology is faster than the pace of regulatory policy updates, and the detailed regulatory rules for new risks such as model risks and data security are not yet sound. The coverage of regulatory sandbox pilot projects is limited [8, 9]. There is also no

established normalized risk information sharing mechanism within the industry, and the risk control experience and risk cases of various banks are difficult to efficiently communicate, which cannot form a cross-institutional collaborative prevention and control pattern, further increasing the difficulty of implementing operational risk management.

6. OPTIMIZATION PATHS OF OPERATIONAL RISK MANAGEMENT OF COMMERCIAL BANKS AMID THE DEVELOPMENT OF FINANCIAL TECHNOLOGY

Starting from the practical goal of deep integration of financial technology and operational risk management, combined with the regulatory norms of the National Administration of Financial Regulation (NAFR) and the practical experience of benchmark institutions in the banking industry, targeted optimization paths for commercial bank operational risk management can be established from four dimensions: technological empowerment, talent construction, internal control reconstruction, and collaborative prevention and control. At the technical level, it is necessary to implement precise allocation of financial technology resources, optimize the intelligent risk control model system, draw on the technical practice of "rule extraction+model distillation" of China Construction Bank (CCB), transform complex neural network models into interpretable and regulable decision-making rules, and strengthen model compliance and operational stability [10]; At the same time, following the fundamental principles of the Data Security Law and the Personal Information Protection Law, A comprehensive data classification and grading management system should be established, increase investment in data security protection technology research and development, and build a solid defense line against data leakage risks from the technical end.

At the level of talent development, it is necessary to establish a system for attracting, nurturing, and retaining interdisciplinary talents. Internally, through financial technology specialized skills training and cross-business line rotation, the technological literacy and risk management practical ability of on-the-job employees should be enhanced; We will accurately expand the scope of campus recruitment and social recruitment, focusing on introducing interdisciplinary professionals in AI, big data analysis and risk management, benchmarking the practical standards of Bank of Communications, gradually increasing the proportion of technology-related personnel to over 8%, and consolidating talent support for the digital upgrade of the risk control system [11]. At the internal control level, it is necessary to reconstruct the institutional system that is adapted to the development of digital business, optimize the internal control process based on the operational characteristics of commercial banks' online business, deeply embed intelligent risk control tools into the entire process of core businesses such as credit and payment, establish a new intelligent early warning mechanism for operational risks, and enhance pre-risk prevention and dynamic monitoring during the process; At the same time, we will enhance the professional capacity of the internal control supervision team, enhance the accuracy and timeliness of risk supervision, and align internal control management with the development of digital business.

At the level of regulation and industry collaboration, commercial banks need to strictly implement the various control requirements of regulatory authorities, actively participate in regulatory sandbox testing, and explore prevention and control models that are adapted to new operational risks; Relying on the industry platform built by the China Banking Association, we will strengthen the exchange and sharing of risk management experience and typical cases among peers, and promote the formation of a new type of operational risk prevention and control synergy in the industry; At the same time, strictly implement the reporting and rectification mechanism for major operational risk events to ensure the timeliness and effectiveness of risk disposal.

7. CONCLUSION

The continuous iteration of financial technology has created a development pattern of opportunities and challenges for the operational risk management of commercial banks. Intelligent technology is gradually replacing traditional manual operations, which not only reduces the scope for human error-related risks, but also significantly improves the overall risk prevention and control efficiency. Along with the deep application of technology, it has also brought about new forms of risks such as data security vulnerabilities, defects in risk control models, and intelligent financial fraud. The insufficient reserves of interdisciplinary talents, inadequate adaptability of internal control systems to digital scenarios, and inadequate regulatory and industry collaboration mechanisms continue to constrain the effectiveness of operational risk management.

Based on the regulatory rules of the National Administration of Financial Regulation (NAFR) and industry practice experience, commercial banks need to carry out operational risk control in accordance with their own digital transformation progress, and reasonably balance the relationship between business innovation and risk prevention and control. Based on regulatory policies and authoritative industry data, we will improve the risk management framework from four directions: technology resource allocation, talent pool construction, internal control system optimization, and industry collaboration and linkage.

By accurately deploying technological resources, cultivating composite financial technology talents, establishing internal control mechanisms adapted to digital business, strengthening interbank communication and regulatory coordination, commercial banks can effectively respond to new operational risks, enhance the capability of operational risk management, and achieve synchronous promotion of digital transformation and stable operation.

This study has certain limitations and insufficient analysis of the differentiated characteristics of operational risk management in small and medium-sized commercial banks. In the future, in-depth research can be conducted based on the development characteristics of banks of different scales, combined with more frontline practical cases, to provide more practical reference ideas for operational risk management of commercial banks.

REFERENCES

[1] Cheng, M., & Qu, Y. (2023). Does operational risk management benefit from FinTech? Emerging Markets Finance and Trade, 59(14), 4012-4027.

[2] Thakor, A. V. (2020). Fintech and banking: What do we know? Journal of financial intermediation, 41, 100833.

[3] Girling, P. X. (2022). Operational risk management: a complete guide for banking and fintech. John Wiley & Sons.

[4] Wang, R., Liu, J., & Luo, H. (2021). Fintech development and bank risk taking in China. The European Journal of Finance, 27(4-5), 397-418.

[5] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

[6] Li, G., Elahi, E., & Zhao, L. (2022). Fintech, bank risk-taking, and risk-warning for commercial banks in the era of digital technology. Frontiers in psychology, 13, 934053.

[7] Chen, B., Yang, X., & Ma, Z. (2022). Fintech and financial risks of systemically important commercial banks in China: an inverted U-shaped relationship. Sustainability, 14(10), 5912.

[8] Feyen, E., Natarajan, H., & Saal, M. (2023). Fintech and the future of finance: Market and policy implications. World Bank Publications.

[9] Omarova, S. T. (2020). Dealing with disruption: emerging approaches to fintech regulation. Wash. UJL & Pol'y, 61, 25.

[10] Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of management information systems, 35(1), 220-265.

[11] Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. Business horizons, 61(1), 35-46.