Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 21, No. 1, 2025

Analysis of New Challenges and Response Paths for Enterprise Risk Management Under the Wave of Financial Technology

Peilin Chen

College of finance, Henan University of Economics and law, Zhengzhou, 450000, Henan, China
772646756@qq.com

Abstract: The in-depth application of technologies such as big data, artificial intelligence, and blockchain in the financial sector has made FinTech a core force driving industry transformation and upgrading. It has not only restructured businesses business models and operational processes but also fundamentally altered the risk environment they operate in. Traditional risk management systems were designed for offline scenarios. Faced with the emerging risks spawned by fintech, they are gradually revealing problems such as lagging risk identification, limited prevention and control measures, and inadequate data security. This article examines the impact of fintech on enterprise risk management and, drawing on the actual operational realities of enterprise digital transformation, identifies emerging risks such as technology dependency, algorithmic bias, and cross-border contagion. It also deeply analyzes the inadaptability of traditional systems, shortcomings in technical security and data compliance, challenges posed by the evolving regulatory environment, and talent gaps. Finally, it offers practical solutions across four dimensions: technology upgrades, system improvements, talent development, and regulatory coordination. These paths aim to provide a reference for enterprises to enhance their risk management capabilities in the context of FinTech and help them achieve stable development amidst the wave of digitalization. Research indicates that enterprises must break away from traditional risk management thinking and build a comprehensive system of "technology + system + talent" to effectively address the various risks posed by FinTech.

Keywords: Fintech; Enterprise Risk Management; Risk Challenges; Response Paths; Digital Transformation.

1. Introduction

Fintech has developed faster than expected in recent years. Mobile payments have permeated offline consumption scenarios, robo-advisors have optimized wealth management processes, and blockchain has resolved the trust challenges of supply chain finance. It has long been deeply integrated into every aspect of business operations. The Peoples Bank of Chinas "China Fintech Development Report (2024)" states that by the end of 2023, the size of my countrys fintech - related market will exceed 15 trillion yuan, with over 500,000 companies leveraging it to improve operational efficiency, with an average productivity increase of over 20%. However, behind these opportunities lies a fundamental shift in the risks businesses face. Previous risk management models were largely "after-the-fact" approaches, relying on manual risk identification. This approach simply cannot keep up with the frequent, hidden, and cross-sector nature of fintech risks. These risks have long since transcended the scope of traditional risk management, making them untenable for traditional models. Current academic research on FinTech and risk management focuses primarily on how to use the technology—for example, the role of artificial intelligence in risk identification—but fails to thoroughly examine the risk challenges posed by FinTech. This is even more evident on the enterprise side, where most prioritize technology adoption over risk prevention and control, and have yet to establish a risk management system adaptable to FinTech. In this context, systematically analyzing the new challenges facing enterprise risk management in the FinTech wave and identifying scientific responses will not only fill gaps in academic research but also provide practical guidance for enterprises. This is highly valuable both theoretically and practically. This article will analyze these challenges from five perspectives: risk profiles, management systems, technological security, regulatory environment, and talent pool, and offer practical solutions.

2. New Enterprise Risk Profiles Driven by FinTech

FinTech has disrupted the boundaries of traditional financial services, transforming the risks faced by enterprises from single-business risks to multi-dimensional, complex risks. Technology dependency, algorithmic bias, and cross-border contagion are the most prominent of these risks, and their intertwined nature significantly increases the difficulty of risk management. Technology dependency is the first hurdle enterprises encounter when using FinTech. Businesses are increasingly reliant on mobile payments, cloud computing, and intelligent algorithms. Failures in these systems can directly impact normal operations. For example, after a retail chain launched mobile payments, the third-party platforms servers suddenly crashed due to excessive load. Thousands of stores nationwide were unable to accept payments for several hours. This resulted in significant revenue losses and complaints from consumers unable to pay, damaging the brands reputation. Even more problematic is "techno logy lock-in." Some logistics companies have long relied on a single service providers big data route optimization system. Later, when the providers technology upgrades failed to keep pace, the company sought a new system, only to discover the enormous costs of data migration and employee training, making the switch unaffordable. Furthermore, if the providers operations were to fail, their own business could be

halted. Algorithmic bias is often caused by poor data quality or flawed algorithmic design. When businesses use tools like intelligent risk control and smart pricing, the algorithms rely on massive amounts of data to make decisions. If the data samples are incomplete or fail to account for specific scenarios, the results can easily be biased. For example, an internet finance company offering microloans used an intelligent risk control algorithm that only considered online consumer data, ignoring offline income verification for migrant workers and self-employed individuals. This resulted in generally low credit scores for these groups, leading to the company losing many potential customers and being summoned by regulators for discriminatory assessments [1]. Furthermore, the algorithm acts like a "black box," making it difficult to explain the decision-making process and quickly identify the root cause. This delays risk management and can even lead to customer complaints. Cross-sector contagion is an inevitable consequence of the "finance + industry" integration of fintech. This "finance + industry" approach has become the norm, allowing risks to spread rapidly across different sectors. For example, an automobile manufacturer relied on a subsidiary finance company to provide consumer loans and also used watermarks to establish a supply chain finance platform to connect upstream and downstream suppliers. Later, due to macroeconomic downturns, car sales declined, consumers were unable to repay their loans, and consumer loan defaults increased. This risk was then transmitted to suppliers through the supply chain platform. Unable to collect outstanding debts, many suppliers experienced funding disruptions, ultimately halting the automobile manufacturers production lines. Traditional risk management, lacking a cross-sector monitoring mechanism, was unable to prevent the spread of risk, ultimately leading to significant losses for the company.

3. The Inadequacy of Traditional Enterprise Risk Management Systems

Traditional corporate risk management systems are a legacy of the industrial age, centered around a vertical model of "departmentalized business management." Whether identifying, assessing, or controlling risks, everything relies on manual effort and experience. However, FinTech has spawned a host of new risks, and this legacy system is no longer able to keep pace. The problems primarily arise in three key areas.

First, risk identification is often slow, failing to capture constantly evolving risks. Traditional approaches rely on manual review of historical data, either monthly or only issuing reports after a risk actually occurs. However, risks evolve so rapidly under FinTech, sometimes causing losses moments after they emerge, making these traditional approaches incapable of responding [2]. Even more problematic, traditional risk identification focuses solely on risks within a single business unit. Risks that involve technology, data, and compliance must also be considered. Because each department is responsible for its own specific areas, without a coordinated leadership role, these risks are often overlooked, leading to potential failures.

Furthermore, risk assessment methods are too simplistic to accurately assess the risks introduced by FinTech. Traditional assessments mostly rely on qualitative analysis, often employing simple quantitative tools like risk matrices. Weightings are determined entirely by the assessors personal experience. However, fintech-specific risks like algorithmic and data risks simply cannot be quantified using this approach. Furthermore, the data used for assessments is almost entirely internal, with no integration of industry risk data or external data related to technical security. This results in an incomplete picture of the risks involved, and the resulting results are naturally far from realistic, failing to provide useful guidance for risk control.

Furthermore, risk control methods are overly rigid and inefficient. Traditional controls rely on either manual intervention or institutionalized processes—for example, multiple layers of approval and restrictions on business scale. These are reactive and slow, unable to keep up with the rapidly evolving nature of fintech risks. More critically, they lack technological assistance. Even when companies have implemented big data risk control systems, they often fail to fully integrate them with existing manual processes. Risk alerts issued by the system are not followed up on, leading to the inevitable bad debts and losses. The risk control system remains largely ineffective, practically useless.

4. Technical Security and Data Compliance Risks in Fintech Applications

Fintechs core lies in technology. For businesses to successfully utilize it, technical security and data compliance are essential foundations—yet these two areas have become the most vexing issues in risk management. Many companies consistently encounter problems in these areas, ultimately stemming from two root causes: a technical architecture that cant withstand risk, and a lack of effective data governance.

A weak technical architecture immediately increases security risks. Fintech relies on cloud computing, big data platforms, and AI algorithms to build a complex framework. If security isnt prioritized during design or if safeguards arent implemented effectively, vulnerabilities are easily left untouched. To reduce costs, many companies favor a "open source technology + third-party services" approach. Open source may appear cheap and flexible, but without code security reviews, hidden vulnerabilities can go undetected. Third-party services also offer far inferior protection levels, leaving the ability to withstand risk largely a matter of luck. Even more problematic, when businesses embark on digital transformation, they often purchase systems from various service providers—for example, one for cloud computing, another for risk control, and yet another for payment systems. These systems lack unified security standards and incompatible data interfaces, resulting in isolated "information silos." If data isnt encrypted when transferred between these systems, it can easily be intercepted and altered, ultimately causing significant losses [3].

With increasingly stringent regulations, data compliance risks are becoming increasingly apparent. Since the implementation of the Data Security Law and the Personal Information Protection Law, data management requirements for businesses have become significantly stricter. However, many companies havent kept pace with compliance, and management remains disorganized. Take data collection, for example. Many companies are obsessed with accumulating more data, either collecting unnecessary information beyond their scope or secretly collecting it without user consent. This completely ignores the principle of "minimum necessary"—

they should collect only what is actually needed. Instead, they seek to collect more than necessary, violating compliance regulations and unnecessarily increasing risks, leaving them scrambling when problems arise. Furthermore, in the storage process, sensitive data is not encrypted and regularly tested for security, leaving servers like unlocked warehouses, easily accessible to hackers. Usage is even more haphazard, with data originally intended for internal credit assessments being transferred to third parties for marketing purposes, completely violating the principle of "purpose-based" data use. Ultimately, not only will regulators summon companies, require them to make corrections, or even impose fines, but their brand image will also be damaged.

5. Regulatory Challenges Faced by Companies in the Fintech Context

Fintech has disrupted traditional business boundaries and accelerated the pace of business model innovation. Traditional regulatory systems struggle to fully cover these challenges, forcing regulators to adjust their strategies and build a dynamic and differentiated regulatory framework. This, in turn, presents new challenges for corporate risk management, primarily in the areas of rapid policy updates, inconsistent standards, and difficulty in cross-border oversight. Frequent regulatory policy updates significantly increase the difficulty for companies to comply. To address the risks associated with fintech, regulatory policies must keep pace with technological advancements and business changes, resulting in frequent and rapid policy adjustments. For example, between 2021 and 2023, my countrys regulatory policies on digital collectibles and virtual currency transactions underwent three adjustments, moving from "trading restrictions" to "complete prohibitions" and then to "regulating technology applications." Even more problematic is that some policies lack foresight and fail to consider the actual adaptation timeframes of businesses. Some payment institutions have received regulatory notices requiring them to complete their "disconnection" transformation within three months. However, this requires replacing core systems and integrating with the China National Network Payment System (CNPS) platform, a task that would take at least six months. This forced businesses to invest additional funds to expedite the process, significantly increasing operating costs. Inconsistent regulatory standards also create a "multiple regulatory" problem. Fintech businesses often operate across multiple sectors, requiring interaction with multiple departments, including the China Banking and Insurance Regulatory Commission, the Peoples Bank of China, and local financial regulatory bureaus. These departments often have inconsistent regulatory standards. To meet compliance requirements, businesses must simultaneously meet multiple sets of standards, naturally increasing compliance costs [4]. Furthermore, regulatory standards vary across regions. For example, a fintech company operating in Province A may require registered capital of 10 million yuan, but this may rise to 20 million yuan in Province B. Further expansion across regions requires additional capital increases, significantly increasing the complexity of business expansion. Cross-border regulation is also a significant challenge, placing significant pressure on multinational corporations. While the borderless nature of fintech facilitates cross-border business operations, regulatory systems vary significantly across countries and regions. Enterprises must simultaneously comply with regulatory rules in multiple countries. For business reporting alone, the frequency and format of submission requirements may differ significantly across different regions. Furthermore, they must meet more stringent customer identification requirements, forcing them to establish dedicated cross-border compliance teams, significantly increasing labor costs. Furthermore, some countries are implementing "data localization" policies. Enterprises with operations in more than 20 countries will need to establish multi-regional data centers, increasing storage costs alone by approximately 30%.

6. Response Paths to Enterprise Risk Management in the Fintech Context

Facing the risks and challenges posed by Fintech, enterprises must break away from traditional mindset and focus on four key areas: technology, systems, talent, and regulatory collaboration. They must establish an integrated risk management system encompassing "technological empowerment, institutional support, talent support, and regulatory collaboration." Technological empowerment is the core of efficiency improvement. Enterprises should develop intelligent risk management systems to achieve "real-time identification, accurate assessment, and dynamic control" of risks. When identifying risks, machine learning should be used to build a real-time monitoring platform that integrates internal transaction data with external industry risk data, significantly accelerating risk identification. For risk assessment, quantitative models should be developed that incorporate metrics such as algorithmic risk exposure and data reliability for more accurate assessments. For risk control, technology should be used to replace manual processes whenever possible to reduce the lag in manual approvals and improve response efficiency. Improving systems is fundamental. Companies should develop risk management systems adapted to FinTech, focusing on technical security and data compliance. Regarding technical security, the "FinTech Technology Architecture Security Standard" should be issued to clarify the testing process for open source technologies and the entry standards for third-party service providers, mitigating technical vulnerabilities at the source. Data compliance should cover the entire process from collection to storage to use, strictly adhering to the "minimum necessary" approach and avoiding excessive collection. Sensitive data should be encrypted during storage and regularly tested for security. Data usage should be clearly defined, and unauthorized transfer is prohibited to prevent data misuse. Talent development is a key support. Companies should build a multidisciplinary team of professionals with both technical and risk management expertise. To address the talent shortage in risk control, we need to recruit more individuals with dual backgrounds in both fintech and risk management to strengthen our risk control teams. Furthermore, we should increase internal training, offering courses on algorithmic risk and data compliance, to help existing risk control personnel enhance their professional capabilities. We can also collaborate with universities and industry associations to establish talent development centers to train specialized professionals and address staffing shortages [5].

Regulatory collaboration can help companies avoid compliance pitfalls. We should proactively connect with regulators, establish regular communication mechanisms, and

promptly address any issues encountered in policy adaptation to avoid crossing red lines due to misunderstandings. We can also engage with industry associations and participate in regulatory policy discussions to understand policy trends early on, allowing ample time for business adjustments. Multinational companies should establish cross-border regulatory response teams to research the requirements of different countries and adapt to local regulations.

7. Conclusion

The rapid development of fintech has brought opportunities for companies to improve operational efficiency and innovate business models. However, it has also exposed them to new risks such as technology dependency, algorithmic bias, and cross-border contagion. Traditional risk management systems are struggling to adapt to these changes. Through analysis, this article found that the core challenges of enterprise risk management are concentrated in four aspects: first, the new risk forms are complex, and traditional identification, assessment, and control methods are lagging behind; second, the technical architecture is fragile and data governance is not standardized, resulting in frequent technical security and data compliance risks; third, regulatory policies are updated quickly and standards are not unified, making compliance more difficult; fourth, the reserve of compound talents in "technology + risk control" is insufficient, which restricts the improvement of risk management capabilities. In response to these challenges, enterprises need to build a response system from four dimensions: technology, system, talent, and regulatory coordination: enable real-time risk identification and dynamic control through technology, and standardize technical security through system improvement. With data compliance management, a composite risk control team is built through talent development, and compliance risks are reduced through regulatory collaboration. Only by breaking the traditional risk management thinking of "departmental division" and "manual dependence" and building a "technology + system + talent" trinity system can we effectively deal with the risks brought by financial technology. This study also has certain shortcomings. For example, it did not analyze the risk differences between enterprises in different industries. In the future, it can combine the characteristics of different industries such as retail, finance, and manufacturing to conduct in-depth research on industry-specific risk management paths. In the future, with the further development of financial technology, new technologies such as quantum computing and the metaverse may bring new risks. Enterprise risk management needs to be continuously iterated to achieve long-term and stable development in the wave of digitalization.

References

[1] Li Yang. Analysis of financing methods and countermeasures for small and medium-sized enterprises under the wave of financial technology [J]. Journal of Inner Mongolia University for Nationalities (Social Sciences Edition), 2018, 44(01): 114-119. DOI: 10.14045/j.cnki.nmsx.2018.01.021.

[2] Ren Kai. Challenges and countermeasures of financial market fluctuations to corporate financial risk management [J]. Enterprise Reform and Management, 2023, (13): 111-113. DOI: 10.13768/j.cnki.cn11-3793/f.2023.0729.

[3] Lv Changshun. Under the suspension of Ant Group's IPO, financial technology companies in the new regulatory era How to plan and respond in the new era [J]. Fortune Times, 2020, (11): 1-3.

[4] Agricultural Bank of China Wuhan Training Institute Research Group, He Duye. Research on the Risk Management Strategy of Small and Micro Financial Services of Commercial Banks in the "Internet +" Era [J]. Journal of Agricultural Bank of China, 2020, (04): 43-48. DOI: 10.16678/j.cnki.42-1864/f.2020.04.009.

[5] Zhu Xiaoyue. Analysis of the Impact of Financial Technology on Small and Micro Enterprises in the Big Data Era [J]. Shopping Mall Modernization, 2022, (02): 98-100. DOI: 10.14013/j.cnki.scxdh.2022.02.037.