

# ***Risk Management of Securities Firms***

**Siyu Chen**

*School of Finance and Investment, Hebei Finance University, Shijiazhuang, China  
18031182601@163.com*

**Abstract.** In the process of transitioning from traditional services to capital intermediation and wealth management, securities firms are facing increasingly complex risks, such as market volatility and credit defaults. Based on this, this study explores the risk management challenges faced by securities companies in the transformation of financial markets. Based on the method of literature analysis, this paper identifies five main risk categories faced by securities firms, namely, credit risk, liquidity risk, operational risk, technical risk and compliance risk, and deeply analyzes the multidimensional nature of risk driving factors, from external shocks to internal defects. This paper innovatively proposes a three-pillar risk management approach: (1) Technology Enablement Pillar, which significantly enhances risk identification transparency through the deployment of artificial intelligence real-time monitoring systems and blockchain regulatory technology solutions; (2) Governance Strengthening Pillar, which relies on the three lines of defense model and forward-looking stress testing to improve the risk management architecture; and (3) Compliance Innovation Pillar, which draws on the Sharia review mechanism of Islamic finance to develop a cross-cultural compliance monitoring system. Chinese securities firms need to upgrade their risk management system architecture. This discovery is not only important for maintaining the stability of the capital market, but also provides Eastern experience for global financial regulatory reform.

**Keywords:** securities risk, fintech, Basel III, compliance, risk governance

## **1. Introduction**

With the deepening development of financial markets, securities companies are shifting from traditional businesses to capital brokers, self-managed investments, and wealth management. As market risk, credit risk, and liquidity risk intertwine, risk types are becoming increasingly complex. The regulatory environment remains tightening, and international regulatory frameworks (such as Basel III) and domestic revisions to the "Securities Law" have placed higher risk management requirements on securities companies [1]. Historical risk events constantly warn of the necessity of risk management, such as the abnormal A-share volatility in 2015 and the Yongmei default in 2020; while the application of Fintech brings opportunities for intelligently controlling risks, it also brings challenges to new issues such as typical risks.

This requires securities firms to strike a balance between business innovation and risk prevention and control, and to establish a more comprehensive and intelligent risk management system.

This study focuses on the new characteristics of risks in the transformation of the securities industry, and innovates risk prevention and control models by using Fintech methods. By analyzing the intertwined impact of traditional risks and technology risks, and combining blockchain technology, it constructs a dynamic risk control system to provide solutions for securities firms' risk control and help optimize regulatory policies.

## **2. The main types of risks faced by securities firms**

### **2.1. Credit risk**

Credit risk, also known as default risk, refers to the possibility that financial institutions will suffer economic losses due to the failure of a counterparty or debtor to fulfill contractual obligations within the agreed period. Credit risk primarily manifests in financing and counterparty-related businesses, encompassing the following aspects: firstly, the insufficiency of customers' margin to cover default losses. Second, the financial party fails to fulfill its share repurchase obligations; third, the counterparty fails in over-the-counter traded derivatives. Finally, creditworthiness deteriorates in bond investments.

### **2.2. Liquidity risk**

Liquidity risk of securities companies refers to the risk that securities companies cannot obtain sufficient funds in a timely manner at a reasonable cost to repay matured debts, fulfill other payment obligations, and meet the funding needs for normal business operations. Liquidity risk includes the liquidity risk of assets and the liquidity risk of liabilities. Asset liquidity risk refers to the risk of assets being able to quickly realize their value. Liability liquidity risk denotes the risk that investment companies face cash shortages, failure to meet debt obligations in a timely manner, inability to cover operating costs, and insufficient liquidity to address large-scale redemptions of the company's managed products by clients—all without inflicting losses on the investment company's assets or clients' assets [2].

### **2.3. Technology risk**

With the advent of the Fintech era, traditional securities business is shifting to the internet, and the introduction of artificial intelligence and blockchain has led to the emergence of new risks. Technological risk denotes the likelihood of losses incurred by securities firms due to information technology system vulnerabilities, cyberattacks, or technical operational errors during their technical operation processes.

### **2.4. Operational risk**

Operational risk refers to the risk of direct or indirectly losses resulting from inadequate or problematic internal operating processes, personnel, systems, or external events, which runs through all business lines or departments of securities companies. For instance, personnel within securities firms may fail to adhere to established procedures, internal systems may experience malfunctions, or external fraudulent activities may be present.

Operational risk emphasizes internal control, and regulations can refer to the "securities firm Internal Control Guidelines" and the "Basic Internal Control Norms for Enterprises."

## 2.5. Compliance risk

According to the "Compliance Management Measures for Securities Companies and Fund Management Companies" [3], which came into effect on October 1, 2017, compliance risk refers to the risk that securities and fund management institutions are held legally liable, subject to regulatory measures, given disciplinary sanctions, suffer property losses or commercial credit losses due to violations of laws, regulations, and norms by the business management or practice of securities and fund management institutions or their employees. In China, compliance risk is mainly governed by regulations such as the "Anti-Unfair Competition Law" [4], with a focus on preventing commercial bribery, data violations, and financial crimes. Regulatory agencies such as the CSRC may impose heavy fines on securities companies that violate regulations.

## 3. Causes of risks in securities companies

Securities firms are confronted with external environmental risks characterized by growing complexity and heightened volatility. In recent years, the A-share market has experienced significant fluctuations. Affected by various international and domestic factors, the stock market has undergone several drastic fluctuations. The market value of the large amount of equity assets and other financial products held by securities companies fluctuates greatly, leading to increased difficulty in realizing assets and rising Liquidity Risk [5]. At the same time, the rise of traditional FinTech has a great impact on securities companies. In recent years, online brokers represented by Robinhood and Futu Securities have attracted a large number of individual investors through zero-commission strategies. In addition, technological innovations such as quantitative trading enable FinTech companies to provide more efficient wealth management, further weakening the traditional competitive advantage of securities companies. In China, some brokerage firms have even fallen into a "price war," with bond listing fees dropping to RMB 700, leading to a decline in profit margins across the industry. Sudden risks cannot be ignored, such as natural disasters, cyberattacks, or geopolitical conflicts. In 2025, an earthquake measuring 8.8 on the Richter scale occurred in Russia, triggering a tsunami that caused short-term turbulence in financial markets, and an earthquake in Japan led to the closure of the Tokyo Stock Exchange. Cybersecurity risks are also serious. Hacking attacks could steal customer data or paralyze trading platforms. For example, during the Russia-Ukraine conflict in 2025, Russia will ban US applications, affecting the cross-border flow of financial information. In addition, global financial regulation is becoming increasingly stringent, with countries introducing stricter compliance requirements, such as China's new asset management regulations and the EU's PSD2 payment directive.

These policies may increase the operating costs of securities companies or restrict their business scope. For example, in 2025, JPMorgan Chase announced that it would charge financial technology companies for data access, which challenged the free model of open banking and may lead to a new round of regulatory review of data cornering the market.

Securities firms are also confronted with internal governance risks, which are primarily manifested in the development of risk management systems and the establishment of internal control mechanisms. Although most securities companies have sufficient strength to build risk management information systems and have indeed invested a lot of money in the construction of these systems, in reality, companies may still encounter problems such as personnel capabilities, technology, operational process design, and hardware and software configuration when building the systems, which affect the stable operation of the company's risk management systems [6]. More critically, some securities firms have significant deficiencies in their internal control management systems,

including unauthorized outflows of funding and resource wastage. This is manifested in the inadequacies of management system design and the gaps in internal processes. This can lead to ineffective monitoring of internal funding flows, inability to guarantee the authenticity of information, and inefficient resource management, thereby increasing market and other financial risks [7].

## **4. Risk prevention and control strategies for securities firms**

### **4.1. Technology driven risk control**

With the acceleration of digital transformation in finance, securities risk management faces challenges such as insufficient transaction transparency and increased fraud risks.

Blockchain and smart contract technologies offer innovative approaches to address these issues. Taking the MasterChain platform tested by the Central Bank of Russia as an example, the Ethereum-based distributed ledger technology enables secure communication and transaction verification between banks. Through smart contracts, pre-defined rules (such as AML/KYC controls and clearing instructions) are automatically executed, greatly improving transaction efficiency and manipulation protection capabilities [8]. In the field of anti-fraud, AI-based monitoring tools (such as ChainAnalysis) can identify high-risk transactions in real time by analyzing on-chain transaction patterns (such as coin mixing behavior and abnormal fund flows), while AI multi-factor risk models used by institutions such as Gold Chain Capital can integrate market volatility.

Liquidity and other data to achieve millisecond-level risk control responses. Furthermore, by incorporating big data analytics (such as analyst attention mechanisms), machine learning can extract historical trading and market sentiment data to help predict stock price crashes or credit default risk. To build a systematic risk control framework, it is recommended to combine the benefits of blockchain data storage with the real-time analysis capabilities of artificial intelligence, for example, by automatically triggering risk elimination through smart contracts (such as account freezing) and creating decentralized insurance funds to share the losses from cyberattacks. Regulators must implement chain compliance tools (such as automated anti-money laundering systems) and dynamically adjust capital buffers in accordance with Basel III standards.

Empirical evidence suggests that Masterchain's communication model and BSVA algorithm can reduce the cross-border transaction costs of securities companies by 78%, while chain monitoring on platforms such as Tronscan (processing 32 million transactions per day) verifies the necessity of artificial intelligence risk control [9].

### **4.2. Strengthen operational management**

Strengthen the "Three Lines of Defense" model to enhance the efficiency and efficacy of risk management. Studies have shown that the principles of integrated quality management and risk management have been significantly strengthened. The three lines of defense contribute to the full effectiveness and efficiency of risk management. Financial institutions should systematically improve the three lines of defense (3LOD) risk management framework: First, strengthen the responsibilities of the first-line business departments and ensure that first-line employees actively identify and manage risks in daily operations through standard operating procedures and integrated risk controls. Second, in order to strengthen the professional capabilities of the second line of defense, the Risk Management Department needs to establish a dynamic monitoring mechanism, use

tools such as stress testing and scenario analysis, and improve risk appetite management and boundary control.

Finally, to ensure the independence of the third line of defense, the Internal Audit Department should adopt a data-driven approach to regularly assess the effectiveness of the first two lines of defense and propose recommendations for improvement. To enhance synergy, institutions should establish horizontal communication mechanisms, conduct joint exercises regularly, link stress test results to line optimization, and ensure real-time sharing of risk information through digital platforms. Simultaneously, senior management should clarify the responsibilities of each line of defense, avoiding functional overlap or gaps, and establish assessment and incentive mechanisms that align with the risk culture.

Introducing stress testing. Stress testing serves as a pivotal tool for financial institutions to evaluate a firm's capital adequacy and risk resilience amid extreme risk scenarios. By simulating shock scenarios such as financial crises, market crashes, or liquidity shortages, stress testing can proactively identify potential vulnerabilities, providing a basis for capital planning and the gradual release of risks [10].

### 4.3. Optimize internal management

The risk rating model is the core tool for securities firms' risk management, requiring the establishment of a six-to-nine-level quantitative scoring system that integrates dimensions such as customer credit, collateral quality, and industry risk. By clearly defining rating standards and dynamically adjusting them every six months, combined with a rating migration matrix to predict default probabilities and expected losses, differentiated risk pricing can be achieved—higher-risk customers should be matched with higher interest rates or margin requirements. The model needs to integrate historical data (such as default records) and forward-looking indicators (policy changes, technology substitution risk), and embed stress tests to assess rating migration under extreme scenarios. For example, the Altman Z-score can provide early warnings of corporate bankruptcy probability, while machine learning can supplement qualitative analysis (such as financial report text sentiment).

Ultimately, RAROC (Risk-Adjusted Return on Capital) is used to balance returns and risks, ensuring the efficiency of capital allocation [11]. Strengthen internal control management and enhance the construction of internal control systems. As the mainstream approach to current internal management, internal control plays a significant role. For the investment banking business of commercial banks, firstly, access management within the market regulatory framework should be implemented to mitigate discrepancies arising from insufficient policy comprehension between regulators and regulated entities. Commercial banks must thoroughly understand various policies and avoid engaging in ambiguous businesses to prevent violations. Second, the management protocols for relevant personnel should be clearly defined to impose constraints on such personnel and establish fundamental operational guidelines [12].

Against the backdrop of accelerating financial innovation, securities firms can draw on the Shariah Supervisory Board's (SSB) independent review mechanism for Islamic banks to establish more effective compliance and risk control systems. Specifically, an interdepartmental "Innovative Enterprise Review Committee" should be established, comprising compliance, risk control, business lines, and external experts, to conduct a "triple review" of innovative enterprises such as derivative product design and cross-border transaction structures. First, the business department submits a rationale for the business. Second, the compliance team conducts compliance checks based on regulatory rules and the company's systems. Third, the risk control unit uses stress tests and scenario



analysis to assess potential risks. The committee must establish a "veto power" to directly halt transactions in cases where regulatory arbitrage or excessive risk spillover is suspected.

Concurrently, an intelligent compliance monitoring system was developed to transform regulatory rules (such as the Measures for the Administration of Cybersecurity and Informatization of the Securities and Futures Industry) into actionable data metrics, achieving a transition from "manual judgment" to "system interception." This dual constraint of "system + technology" ensures that innovation does not exceed limits and risks do not spill over [13].

## 5. Conclusion

This study systematically analyzes the five major categories of risks faced by securities companies in the transition to capital intermediaries and wealth management, including Credit Risk, Liquidity Risk, operational risk, technological risk, and compliance risk. It deeply analyzes the internal and external drivers behind these risks, encompassing external factors such as heightened market volatility, intensifying industry competition, the impact of unforeseen incidents, and increasingly rigorous regulatory policies, as well as internal inadequacies including deficiencies in risk management systems and flaws in internal control mechanisms.. In response to these risk challenges, the study innovatively proposes a risk prevention and control system based on three pillars: technology empowerment, governance enhancement, and compliance innovation. It recommends building a more intelligent, efficient, and forward-looking risk management framework through measures such as real-time monitoring with artificial intelligence, application of blockchain technology, optimization of the three-lines-of-defense model, strengthening of stress testing, and construction of cross-cultural compliance mechanisms.

The research not only provides practical guidance for securities companies to enhance their risk management capabilities but also offers a theoretical reference for regulatory authorities to improve risk prevention and control policies, which is of great significance for promoting the balanced development of the securities industry between innovation and stability. Future research may further focus on the synergistic mechanism of regulatory technology and systemic risk early warning, as well as the prevention and control paths of cross-border risk contagion, and other directions.

## References

- [1] Basel Committee on Banking Supervision. (2010). Basel III: A global regulatory framework for more resilient banks and banking systems. Bank for International Settlements. <https://www.bis.org/publ/bcbs189.htm>
- [2] Kumar, Manish, and Ghanshyam Chand Yadav. "Liquidity risk management in bank: a conceptual framework." AIMA journal of management & research 7.2/4 (2013): 0974-497
- [3] China Securities Regulatory Commission. Measures for the Compliance Management of Securities Companies and Fund Management Companies (CSRC Order No. 133) [EB/OL]. (2017-06-09) [2023-11-20]. <http://www.csrc.gov.cn/csrc/c101862/c1629951/content.shtml>
- [4] National People's Congress. (2019). Anti-Unfair Competition Law of the People's Republic of China (Amended 2019). <http://www.npc.gov.cn/englishnpc/c23934/202001/0a70c6ac7f744b87a7e60e7d2a5a9d0c.shtml>
- [5] Zhang, Jing. "Analysis of Liquidity Risk of Securities Companies under the Current Policy Background." Market Weekly 37.28 (2024): 123-126.
- [6] Wu, Weiyan. "Research on Liquidity Risk Management of Securities Companies under the New Regulatory Background." Market Weekly 37.18 (2024): 49-52.
- [7] Zhao, Linna. "Research on Enterprise Financial Risk Prevention and Control." Vitality 43.12 (2025): 151-153.
- [8] Mishchenko, Svitlana, et al. "Innovation risk management in financial institutions." Investment Management and Financial Innovations 18.1 (2021): 191-203.
- [9] Wang Yong, et al. "Challenges and Countermeasures of Securities Company Risk Management under the Innovation Situation". Innovation and Development: Collection of Papers on China's Securities Industry 2015. Ed.

Everbright Securities Co., Ltd.; 2015, 159-165.

- [10] Aloqab, Abdullab, Farouk Alobaidi, and Bassam Raweh. "Operational risk management in financial institutions: An overview." *Business and economic research* 8.2 (2018): 11-32.
- [11] Reddy, G. Divakara, and M. Thaiyalnayaki. "Risk management in investment banking." *International journal of health sciences* 6.S1 (2022): 12975-12988.
- [12] Deng, J. Y. "Research on Risk Management of Investment Banking Business of Commercial Banks in China." *Business Information*. 31 (2021): 83-85.
- [13] Al Rahahleh, Naseem, M. Ishaq Bhatti, and Faridah Najuna Mismam. "Developments in risk management in Islamic finance: A review." *Journal of Risk and Financial Management* 12.1 (2019): 37.