Risk Identification of Enterprise Artificial-Intelligence Applications from the Perspective of Socio-Technical System Theory: Evidence from OECD AI Incident Monitor and Representative Cases

Haoshu Lu

School of Economics and Management, Changsha University of Science and Technology, Changsha, 40100, Hunan, China
2296740839@qq.com

Abstract. Against the backdrop of artificial-intelligence-driven financial digital transformation and improving industrial regulatory rules, the popular application of artificial intelligence in corporate financial accounting, risk-control decision-making and capital-market transactions has given rise to new-form financial risks, rendering traditional governance frameworks inadequate. Taking listed-company artificial-intelligence-based financial risk governance as the research subject, this paper adopts data coding statistics and case-study methods. Drawing on 175 valid samples from the OECD artificial-intelligence financial-risk incident database and positive-negative comparative cases of eight Chinese listed firms, this study applies the Socio-Technical System Theory and the Basel Operational Resilience Framework. It reconstructs a financial-risk system adapted to artificial-intelligence scenarios and establishes a multidimensional collaborative risk-governance mechanism. This research mitigates fragmented research perspectives and insufficient empirical evidence in existing literature, and provides theoretical reference and practical suggestions for Chinese listed companies to guard against AI-related financial risks, advance digital transformation while controlling risks, and improve intelligent-financial governance systems.

Keywords: Artificial Intelligence; Financial Risk; Basel Risk Classification; Socio-Technical System Theory; Operational Resilience

1 Introduction

Artificial intelligence has been fully integrated into financial accounting, credit risk control and capital-market businesses of listed companies, accelerating digital transformation in the financial industry. In July 2023, seven Chinese regulatory authorities issued the Interim Measures for the Administration of Generative Artificial Intelligence Services. While encouraging AI technological innovation, the document requires AI service providers to implement content review, data compliance and risk-assessment mechanisms. It imposes strict norms for model application in high-precision finan-

© The Author(s) 2026
B. P. Siba et al. (eds.), *Proceedings of the 2026 5th International Conference on Public Service, Economic Management and Sustainable Development (PESD 2026)*, Advances in Economics, Business and Management Research 411,
https://doi.org/10.2991/978-94-6239-825-2_54

cial-accounting scenarios to curb potential hazards such as algorithm bias and information distortion. In August 2025, the State Council released the Opinions on Further Implementing the "AI+" Initiative. It promotes in-depth integration of artificial intelligence with finance and accounting, and urges enterprises to build full-lifecycle AI risk-prevention systems. Review and fault-tolerant mechanisms shall be improved for intelligent financial-report generation, intelligent risk control, investment-financing decision-making and other scenarios, setting compliance boundaries for industrial development.

Driven by policy support and technological popularization, new financial risks keep emerging as enterprises deploy artificial intelligence on a large scale. AI-related financial risks have evolved from mere technical hazards into quantifiable and transmissible operational and capital-market risks. Without targeted management-control systems, such risks will continuously undermine corporate financial soundness and threaten the stable operation of capital markets.

2 Literature Review and Theoretical Basis

2.1 Literature Review

Domestic and overseas scholars have developed three major research strands regarding AI-related financial risks: technological-application effects, risk-formation mechanisms and governance-mechanism construction. Nevertheless, existing research suffers from insufficient theoretical integration, simplistic risk attribution and scarce empirical evidence based on local cases.

In terms of technological-application effects, Hou X. (2025) contends that AI-driven digital transformation of enterprise financial accounting should transcend routine operational optimization and evolve toward strategic decision support, achieving enhanced efficiency, risk prevention, and value creation[1]. Chen H. (2026) further argues that AI-enabled financial management transformation extends beyond accounting automation to functional boundary expansion and behavioral evolution, with large-model technologies profoundly impacting operational interaction, business processes, data analytics, and knowledge management[2]. Chen L. (2025) points out that generative AI applications in corporate financial reporting raise governance dilemmas, necessitating a clear delineation between technological tools and financial liabilities[3]. Li J et al. (2025) empirically find that the risks and benefits of corporate AI adoption largely depend on internal dynamic governance capabilities[4].

Regarding risk alienation and transmission, Zhao et al. (2025) demonstrate that corporate AI adoption paradoxically elevates stock price crash risk through information asymmetry and managerial opportunism[5]. Dong et al. (2026) show that AI technology accessibility significantly promotes firm growth across total assets, tangible assets, and market capitalization, yet larger firms reap disproportionately greater benefits, widening the growth gap between large and small enterprises[6]. Elouadi & El Bouanani (2026) emphasize that AI transforms economic forecasting by processing vast data to uncover complex patterns for more accurate predictions, while cautioning that model opacity may introduce systematic biases[7]. Li X. (2025), through an empirical study of

235 SMEs, finds that generative AI improves risk identification accuracy by 27.3% and prediction precision by 34.5%, with technology acceptance, data quality, and organizational support serving as critical moderators[8]. Han, Wu & Li (2026) reveal that AI adoption increases firm risk-taking by strengthening absorptive, adaptive, and innovative capabilities, an effect more pronounced among firms with low ESG performance, in low-technology industries, and in less marketised regions [9].

On risk governance, Zhang & He (2025) apply Socio-Technical System Theory and conclude that AI-induced risks arise from multifactor interactions and cannot be eliminated through algorithm optimization alone [10]. Crisanto & Mangano (2024) introduce operational-resilience concepts and advocate a comprehensive pre-event-in-event-post-event prevention-control framework [11]. Blum & Raviv (2026) demonstrate regional heterogeneity in risk-reporting behaviour under Basel III through topic modeling of large banks' financial reports [12]. Yin H et al. (2025) further note that machine learning techniques carry inherent uncertainty, and risk governance should not be confined to algorithmic improvements [10].

To sum up, abundant literature exists yet research perspectives remain fragmented. Few studies investigate risk transmission and management-control systems based on domestic corporate samples. Accordingly, this paper reconstructs scenario-oriented classification for traditional financial risks, analyses AI-related financial risks from a multidimensional-adaptation perspective, combining OECD risk-incident samples and positive-negative A-share case studies to fill existing-research gaps.

2.2 Theoretical Basis

The Socio-Technical System Theory suggests that technology cannot function independently. Risks stem from interactions among technology, human agents, organizations, procedures and external environments. It supports systematic analysis of multiple inducing factors behind AI-related financial risks. The Basel risk-classification system and Operational Resilience Framework are authoritative instruments for financial-risk management, enabling iterative analysis of traditional risks and research on risk-blocking paths under AI scenarios. Complementing each other, the two theories: the former explains risk origins; the latter focuses on governance optimization. Together they build the theoretical framework for studying the mechanisms and countermeasures of AI-related financial risks.

Rejecting technological determinism, Socio-Technical System Theory emphasizes joint optimization of technical and social subsystems, which has been widely adopted in digital-transformation risk research. Domestic scholars have verified that digital risks mostly originate from multifactor adaptation imbalance, providing an analytical paradigm for this paper’s risk identification.

Successively revised since 1988, the Basel Accords established the eight-category financial-risk-classification system covering credit risk, market risk, liquidity risk, operational risk, legal risk, reputational risk, strategic risk and systemic risk, which serves as the global benchmark for financial-risk regulation. As artificial intelligence penetrates financial-accounting workflows, the connotation, boundaries and transmission paths of traditional eight major risks have undergone subversive changes. Original

management frameworks can no longer accommodate new-risk features, which provides the theoretical ground for this paper's reconstruction of scenario-specific AI financial-risk systems.

Basel II centres on post-hoc loss recording and capital provisioning, which only suits manual-based traditional financial businesses and fails to address digital risks such as algorithmic disturbance and system anomalies. Released in 2021, the Principles for Operational Resilience establishes new regulatory logic. Abandoning the objective of "complete risk elimination", it constructs a full-chain mechanism: pre-event identification & protection, in-event adaptation & interruption, post-event recovery & review. It highlights business continuity and emergency-response capacity amid risk disruptions and supplies new ideas for governing new-type AI risks. Domestic research further confirms that operational-resilience logic fits the uncertainty and quantification difficulty of large-model risks[3]. Given the chain-propagation and sudden-perturbation features of AI-related financial risks, the full-chain governance logic offers solid theoretical support for studying risk-blocking and governance paths.

Accordingly, this paper analyses artificial-intelligence-related risk incidents and corporate cases from multiple dimensions. Drawing on the Socio-Technical System Theory, it identifies five hazard-inducing analytical dimensions: technology, personnel, organisation, business procedures and external environment. Combined with the Basel Operational Resilience Framework, the dimension of regulatory resilience is further added to form a unified six-dimensional analytical framework. This framework is applied both to multi-label coding and statistical analysis of 175 overseas AI-risk incidents from the OECD database, and to the comparative decomposition of positive and negative cases of eight domestic A-share listed companies. Balancing macro large-sample incident statistics and micro local-case evaluation, this paper identifies common hazard-inducing factors behind artificial-intelligence-driven financial risks and dissects risk formation and transmission logic through macro-micro cross-verification.

3 Research Design

3.1 Data Sources and Sample Screening

Data and case materials of this paper are obtained from the OECD database (https://oecd.ai/en/incidents), annual reports of A-share listed companies, regulatory announcements released by the China Securities Regulatory Commission and authoritative financial-news media. All data are publicly traceable and comply with social-science case-study norms. The OECD database is an internationally authoritative fintech-risk-research repository collecting global AI-related financial-risk incidents and compliance defects. Annual reports and regulatory announcements reflect corporate AI investment, asset impairment, compliance penalties and other operational facts to guarantee authenticity and rigour.

Python crawler tools retrieved 1441 original risk samples from the financial-insurance sector in the OECD database (cutoff date: 11 August 2025). After manual screening, 175 valid samples highly relevant to listed-company AI financial

risks were retained. The samples cover A-share key industries including AI technology, fintech and high-end manufacturing, involving scenarios such as computing-power investment, intelligent-finance application, algorithm-driven risk control, asset impairment and information-disclosure anomalies.

3.2 Selection of Typical Cases

Four A-share firms are selected as negative cases: Kunlun Tech, TRS Information Technology, Yanshan Technology and Etown Intelligent. They represent native-AI tech enterprises, traditional-software-transformed firms and manufacturing enterprises cross-border into AI business. Their cases reflect common financial hazards caused by blind AI expansion: sunk costs in computing infrastructure, goodwill impairment, cash-flow pressure and nonstandard information disclosure.

Four listed banks are chosen as positive cases: Bank of China, Bank of Ningbo, China Merchants Bank and Industrial and Commercial Bank of China. Subject to strict financial supervision, domestic banks have taken the lead in deploying enterprise-grade AI risk-control platforms, standardized human-machine-collaboration mechanisms and full-process resilience-governance systems. They mitigate model-defect-induced financial risks and realise cost reduction plus risk mitigation. Positive-negative comparisons highlight risk divergence arising from heterogeneous AI-governance performance and compensate for the localization shortcoming of overseas OECD samples.

3.3 Research Analytical Dimensions

Based on the Socio-Technical System Theory, the Basel Operational Resilience Framework and characteristics of samples and cases, six analytical dimensions are defined: technology, personnel, organization, procedure, external environment and regulatory resilience. The first five dimensions derive from Socio-Technical System Theory for analysing risk-inducing factors. The regulatory-resilience dimension is built upon the Basel Operational Resilience Framework to study risk resistance, transmission blocking and governance optimisation. The six dimensions apply consistently to both macro-sample statistics and micro-case decomposition, supplying a unified analytical framework for risk-mechanism analysis and governance-solution construction.

4 Data Analysis

This chapter conducts empirical analysis on 175 independent risk incidents (2021-2026) from the OECD AI Incident Monitor. Note that the database collects risk-oriented incidents rather than random samples; statistical outcomes only reveal risk patterns instead of real-world industry incidence. Multi-label text coding is performed across four perspectives: sample descriptive statistics, five-dimensional hazard-factor distribution, risk-task characteristics and operational-resilience insights to provide empirical evidence for risk reconstruction and subsequent case analysis.

4.1 Descriptive Statistics of Samples

All the 175 samples from financial-insurance scenarios involve property and economic damage (100%), proving that AI-related financial risks ultimately translate into corporate economic losses. Secondary consequences include reputational damage (61.1%), violation of human rights and interests (47.4%), harm to public interests (34.9%) and psychological harm (34.3%). Extreme fatal incidents are extremely rare. It demonstrates that AI-related financial risks are multilayered compound hazards accompanied by reputational and public-interest spillover effects.

In terms of AI task categories, content-generation tasks account for the highest risk proportion (96 cases, 54.9%), constituting the primary risk source in financial-accounting scenarios, followed by goal-driven operational tasks (55 cases, 31.4%) and intelligent interactive Q&A tasks (43 cases, 24.6%). Risks originate from dual channels: internal large-model malfunctions and external malicious fraud perpetrated via artificial-intelligence tools.

Regarding system autonomy: high-autonomy-system risks 70 cases (40.0%); no-autonomy-system risks 59 cases (33.7%); low-autonomy 32 cases (18.3%); medium-autonomy 14 cases (8.0%). Statistics indicate risk severity does not correlate absolutely with system autonomy. Even AI tools without operational authority may trigger substantial financial losses if their outputs are improperly adopted by humans. Judging risk levels merely by human-participation intensity has obvious limitations.

Risk-affected subjects: consumers 111 cases (63.4%); enterprises themselves 75 cases (42.9%); general public 41 cases (23.4%); employees 25 cases (14.3%), reflecting cross-subject risk diffusion. The 41.1% proportion of U.S. samples results from English-media-collection bias and does not represent real regional risk levels.

4.2 Coding Analysis Based on Socio-Technical System Theory

Table 1. Five-dimensional Risk Distribution Statistics

Analytical Dimension	Cases Hit	Percentage
Technology	146	83.4%
Personnel	130	74.3%
Organization & Institution	124	70.9%
Business Procedure	130	74.3%
External Environment	132	75.4%

As shown in Table 1, high risk coverage exists across all five dimensions. No single dimension dominates risk generation, verifying the compound multifactor-coupling nature of AI-related financial risks and furnishing empirical grounds for analysing risk pain points and building governance systems.

The technology dimension registers the highest hit ratio and acts as the major risk trigger, covering model defects, data vulnerabilities and misuse of synthetic content. Co-occurrence between technology and organization / business-procedure dimensions both reaches 66.3 %; 70.9 % of incidents hit four or more dimensions; 50 incidents cover all five dimensions.

Statistics confirm AI-related financial risks seldom stem from isolated technical breakdowns. Technology serves only as the trigger. Whether latent hazards evolve into tangible losses hinges on joint adaptation of human supervision, organizational governance, procedural control and external conditions, which validates core arguments of Socio-Technical System Theory. (Table 2).

Table 2. Breakdown of Core Risk Indicators in Each Dimension

Analytical Dimension	**Valid Samples**	**Core Risk Indicators (Percentage)**	**Summary of Risk Characteristics**
Technology	146 cases	1.Automated-decision & model risk (52.1%) 2.Identity forgery & synthetic-content abuse (42.5%) 3.Cybersecurity & system vulnerability (39.0%)	Automated-link loopholes and malicious-content abuse constitute more important technical triggers. Technical defects are merely initial triggers rather than exclusive causes of risk outbreaks.
Personnel	130 cases	1.Interest infringement & unfairness (90.0%) 2.Absence of human supervision & failure of accountability (59.2%) 3.Human agents misled by AI outputs (51.5%)	Over-reliance on algorithms and weakened professional judgement are core pain points. Missing human intervention magnifies technical deviations and converts latent risks into real losses.
Organization & Institution	124 cases	1.Unclear algorithm accountability & insufficient transparency (77.4%) 2.Absence of compliance management & policy enforcement (62.9%) 3.Deficient data governance & internal-control authority (52.4%)	Deficient enterprise-specific AI-governance institutions and blurred accountability create institutional loopholes that fuel repeated AI-financial-risk outbreaks.
Business Procedure	130 cases	High-risk workflows: customer-account maintenance, IT R&D roll-out, credit-transaction pricing Key flaws: lack of review, fusing and roll-back mechanisms for intelligent workflows	Defective business procedures fail to correct minor technical deviations, enabling cascading amplification into large-scale financial losses.
External Environment	132 cases	Key risk drivers: social-public disturbance, regulatory updates, external malicious attacks, infrastructure dependence	Fluctuations in external ecosystems magnify internal corporate-control weaknesses and accelerate risk spill-over.

4.3 Risk Reconstruction Based on the Basel Framework

Table 3. Renaming and Re-definition of Risks under Basel-Framework Scenario Adaptation

Traditional Risk Name	Re-named Risk	Core Re-defined Risk Points
Credit Risk	AI External Forgery Attack Risk	Deep-fake generated false credit materials, model poisoning interfering risk-control judgements, theft of corporate financial-credit data, inducing credit default and intelligent fraud.
Market Risk	Intelligent Procedure Conduction Solidification Risk	Insufficient fault tolerance of AI trading-valuation workflows plus absent human review. Algorithm-deviation propagation; algorithm homogenization amplifies stock-price and interest-rate volatility.
Operational Risk	Internal AI Intelligent Fraud Risk	Insiders exploit large-model vulnerabilities to tamper with financial reports, conduct algorithm arbitrage and manipulate intelligent-finance systems, producing concealed internal operational violations and fraud.
Liquidity Risk	Computing-Power Hardware Damage Risk	Breakdown of computing-power servers and AI-infrastructure halts intelligent accounting and capital-scheduling, triggering corporate capital-turnover failure.
Legal Risk	AI Intelligent-Business Compliance Risk	Biased model outputs and non-standard workflows produce financial-report-disclosure defects and business non-compliance, leading to legal-compliance consequences in finance-accounting fields.
Cross-border Risk	AI Governance and Ecosystem Fluctuation Risk	Overseas computing-supply-chain dependence, cross-border AI-regulatory divergence and global fin-tech-ecosystem volatility induce cross-border risk transmission.
Reputational Risk	Large-Model Iteration Failure Risk	Abnormal large-model iteration and compatibility failures cause erroneous financial disclosures and large-scale business outages, triggering public-opinion crises and reputational damage.
Strategic Risk	Human-Machine Collaboration Mismatch Risk	Blind investment in AI computing-power R&D, blurred human-machine rights-obligation boundaries and lagging governance construction produce resource misallocation, decision bias and goodwill-impairment strategic losses.

Basel II risk design fits manual-mode finance and relies on post-hoc loss statistics and capital provisioning. It cannot accommodate the uncertainty, concealment and correlation of AI risks. Some enterprises with sufficient capital reserves still suffer fraud

losses, business interruptions and market swings due to inadequate procedure control, human-machine review and emergency response; capital provisioning alone cannot contain new-form AI risks. In addition, multi-risk superimposition renders static traditional risk classification insufficiently explanatory.

Retaining the classic eight-category Basel risk framework, this paper renovates connotation, scenarios and core pain points according to real-world risk-incident features to reconstruct scenario-adapted financial-risk typology for AI-enabled finance.

Table 3 realises accurate adaptation and upgrading from traditional financial risks to new AI-related financial risks. It clarifies brand-new manifestations and hazard drivers under intelligent-finance scenarios and furnishes standardized criteria for case risk attribution and governance-path construction.

4.4 Insights Derived from Data Analysis

First, AI-related financial risks are typical socio-technical configurational risks instead of purely-technical hazards. Technology serves as a primary trigger, yet multidimensional adaptation imbalance constitutes the root cause of risk outbreaks. Pure algorithm optimisation cannot resolve risks; coordinated improvement across personnel, organisation, procedure and external environment is indispensable.

Second, risk assessment cannot depend on system-autonomy level. AI tools without operational authority can still produce heavy financial losses under human misuse or external abuse. Risk management should focus on permission configuration, substantive human supervision and emergency-correction-mechanism construction.

Third, content-generation scenarios represent high-risk territory. Risks propagate via internal-defect and external-malicious-abuse dual channels. Besides economic losses, reputational and public-interest harms are prominent; governance needs to address multiple risk consequences.

Fourth, traditional post-hoc capital-oriented control proves inadequate. The full-chain philosophy of Basel operational resilience better fits AI-risk characteristics. Enterprises ought to establish complete resilience-governance workflows covering pre-event prevention, in-event interruption and post-event review.

OECD dataset mainly covers overseas negative incidents with limited local A-share samples. Therefore eight domestic-listed-company positive-negative cases are introduced to enhance conclusion applicability.

5 Case Analysis

OECD macro-level samples are mostly overseas incidents with limited adaptability for Chinese A-share enterprises. To remedy localization weaknesses, eight A-share listed companies are selected for comparative-case study: four leading banks as positive cases and four domestic tech-manufacturing enterprises as negative cases. The six-dimensional analytical framework is adopted to unpack AI-empowerment mechanisms and risk causes and realise mutual verification between macro laws and micro-level practical experience.

5.1 Analysis of Negative-Case Influencing Factors

Four cross-industry A-share negative cases are studied: Kunlun Tech, TRS Information Technology, Yanshan Technology and Etown Intelligent. They cover native-AI tech firms, internet-transformed enterprises, digital-service providers and traditional manufacturers undertaking AI cross-border transformation, reflecting common governance defects during domestic AI-financial digital transformation.

Table 4. Comparison of Common Risk-Influencing Factors

Dimension	Common Factor	OECD Risk Samples	Negative Domestic Cases	Summary of Common Risk
Technology	Model defects & automated-decision risks	52.1% of samples suffer automated-decision-model risks including model drift and algorithm bias as primary triggers	Blind adoption of off-the-shelf large models; unstable self-developed-model iteration; mismatch between computing-power investment and practical outcomes	Technical uncertainty constitutes precondition for risks; model defects and automated-link vulnerabilities serve as core technical triggers of AI-financial risks.
Personnel	Absent human supervision & failed professional judgement	59.2% cases lack human supervision and accountability; 51.5% witness staff misled by AI outputs and algorithm over-reliance	Insufficient AI literacy among finance staff; lack of professional judgement and review awareness; missing human-machine-collaboration mechanisms that cannot offset technical biases	Over-reliance on algorithms and inadequate professional competence amplify technical defects and turn latent risks into tangible financial losses.
Organization & Institution	Lagging governance & blurred power-responsibility boundaries	77.4% cases feature ambiguous algorithm accountability and transparency; 70.9% hit organisational-institution dimension with missing dedicated AI-governance rules	AI strategy decoupled from internal control; absence of special AI-application-management systems; blurred authority boundaries among tech-business-risk-control departments; hollow accountability	Lagging organisational governance behind AI-technology progress constitutes the root cause of corporate AI-financial risks.
Business Procedure	Deficient intelligent-business procedural control	Intelligent workflows lack review, fusing and roll-back mechanisms; minor technical deviations	Absent pilot-verification and risk investigation before AI-business launch; missing hu-	Imperfect procedural control forms the core transmission channel for risks to expand

Dimension	Common Factor	OECD Risk Samples	Negative Domestic Cases	Summary of Common Risk
		cascade into large-scale financial losses	man-review links for intelligent accounting and computing-power management; risks cannot be intercepted in advance	from isolated defects to systemic financial losses.
External Environment	External-ecosystem turbulence & malicious attacks	75.4% of samples hit external-environment dimension: malicious external attacks, regulatory iteration and infrastructure dependence magnify internal control weaknesses	Dependence on external vendors for computing-power supply; slow corporate compliance adjustment amid regulatory updates accelerates risk spill-over	Uncertainties in external environments amplify internal corporate-governance deficiencies.
Governance	Multi-dimensional adaptation imbalance	70.9% incidents hit four or more dimensions; 50 incidents cover all five dimensions	Technology-investment rhythm outpaces supporting-governance construction; comprehensive adaptation imbalance across technology-personnel-organisation-procedure-environment	AI-related financial risks are not purely-technical problems but compound risks caused by multi-dimensional adaptation imbalance; the degree of governance adaptation determines ultimate risk impact.

Kunlun Tech invested heavily in AGI R&D and computing-power ecosystems but failed to build matching internal-control and human-machine review institutions. Heavy computing-power spending squeezed cash flow. Unstable model iteration and poor commercialisation brought asset impairment and performance volatility.

TRS Information Technology deployed AI-driven intelligent accounting and risk-control applications, yet technological iteration outpaced workflow upgrade and staff competence. Blind promotion of fully-automatic financial workflows weakened human review. Large-model hallucinations created financial-data flaws and long-term compliance hazards.

Yanshan Tech relied heavily on third-party general-purpose large-models without self-built data-security systems. External-model instability and interface vulnerabilities frequently occurred. Absent procedural-fusing mechanisms and dedicated AI governance accumulated operational-compliance risks.

Etown Intelligent represents traditional manufacturers with AI cross-border investment. Finance teams lacked AI literacy; intelligent-finance systems went online without sufficient risk assessment, resulting in cost-accounting bias. Large AI capital expenditure squeezed operating cash flow.

All four firms share the core problem: technical input outpaces supporting governance construction. Risks are compound risks from adaptive imbalance across multiple dimensions. Table 4 compares risk-inducing factors between OECD samples and domestic negative cases.

5.2 Analysis of Positive-Case Influencing Factors

This paper unpacks AI-governance and risk-mitigation mechanisms of four banking positive cases from six dimensions.

From the technical perspective, banks adopt platform-based compliant deployment. They build self-controllable enterprise-grade AI risk-control platforms rather than directly applying general-purpose large models. Bank of China independently develops the BOCAI intelligent platform. China Merchants Bank constructs mixed basic-and-vertical-domain model matrix. Industrial and Commercial Bank of China leverages the ICBC Intelligent Surge platform. Platform-oriented architecture mitigates model drift, data contamination and algorithm black-box risks.

In terms of personnel, banks implement standardized human-machine collaboration systems. China Merchants Bank carries out enterprise-wide AI-literacy training and job certification. Industrial and Commercial Bank of China incorporates AI-risk identification into routine training. Bank of Ningbo sets up risk-control expert panels participating in model design and testing. Human professional judgement compensates model deviations.

From the organizational perspective, special AI-governance structures clarify rights and responsibilities. Banks formulate AI governance guidelines, connect AI strategy with compliance-risk-control systems, and build multi-department collaborative frameworks to balance technological innovation and risk restraint.

As for procedures, banks adopt pilot-verification, phased-iteration deployment instead of one-off large-scale roll-out. AI tools are embedded into segmented business links. Scenario-based pilots identify potential hazards before large-scale promotion and block chained risk transmission.

In the dimension of external environment and regulatory resilience, banks keep pace with regulatory updates, conduct regular AI-model stress tests, and build emergency-recovery mechanisms for business disruptions to cope with policy and ecosystem uncertainties.

5.3 Mechanisms and Governance Approaches

Positive-case risk-control empowerment stems from multidimensional synergy: compliant technical deployment lays foundations; specialist personnel compensate for model weaknesses; clarified organisational authority defines application boundaries;

iterative-procedure deployment mitigates latent risks; adaptive external compliance sets bottom lines; full-chain regulatory resilience blocks risk diffusion.

By contrast, negative-sample enterprises show “aggressive technical investment with lagging supporting governance”. Their risks stem from governance lag behind technical iteration rather than pure AI-technology defects.

Table 5. Summary of Governance Mechanisms and Experience for Case Enterprises

Dimension	Positive Effect	Governance Experience
Technology	Platform-oriented specialisation and governability reduce model biases	Build enterprise-grade platforms; unify data standards; implement full-life-cycle management.
Personnel	AI literacy and professional judgement realise cognition absorption and bias correction	Enterprise-wide AI training; risk experts participate in model design and approval.
Organisation	Strategic consistency plus three lines of defence realise innovation and checks-and-balances	Embed AI into corporate strategy; clarify authority for technology, business, risk-control and audit departments.
Procedure	Business embedding plus MVP pilot expose risks in advance	Adopt MVP pilot; establish workflow of "AI processing + human review + anomaly interception".
External Environment	Clear regulation and open-source ecosystems lower uncertainty	Dynamically adapt to regulatory rules; participate in open-source communities and industrial cooperation.
Regulatory Resilience	Continuous monitoring, stress-testing and business continuity block risk propagation	Build AI-risk inventories; conduct stress-tests; formulate emergency suspension and exit contingency plans.

Table 5 establishes a complete governance chain: technology as foundation, personnel empowerment, organisational checks-and-balances, procedural implementation, environmental adaptation, resilience as safety net. It supplies practical pathways for listed companies to construct AI-financial-risk-governance frameworks.

6 Research Conclusions

Synthesizing overall-research procedures, sample statistics and case judgements: risk-performance and practical outcomes of artificial intelligence within corporate-finance scenarios show obvious governance-dependent features. Technology itself is not the sole determinant of risk magnitude or value output. According to multidimensional coding statistics based on 175 AI-financial-risk valid samples,

AI-financial-risk formation correlates broadly with adaptive imbalance across technology, personnel, organisation-institution, business-procedure and external-environment dimensions, all showing high risk-coverage ratios. This proves intelligent-financial-risk formation results from combined multifactor effects.

The traditional eight-category Basel financial-risk system was built for manual-mode finance. It cannot adapt to large-model iteration, intelligent automatic-decision-making and deep human-machine-collaboration scenarios. Accordingly, this paper renovates the Basel risk-classification system and defines scenario-specific risks such as AI external-forgery-attack risk, intelligent-procedure-conduction-solidification risk and human-machine-collaboration-mismatch risk. It realises scenario-oriented upgrading for classic regulatory frameworks.

Evidence from four domestic-listed negative-case studies shows that during AI-intelligent-transformation, these firms all suffer misalignment: technical-investment rhythm outpaces internal supporting-governance development. These deficiencies trigger tangible-financial consequences such as computing-power-asset impairment, inefficient R&D-resource allocation, financial-compliance defects and squeezed corporate operating cash flow. This fully proves that inadequate multidimensional governance adaptation constitutes the core inducement for corporate AI-financial risks.

In sharp contrast, the four listed-bank cases reflect positive application value brought by artificial intelligence under sound institutional constraints, standardised procedural control, specialist-personnel capacity and stable regulatory ecosystems. Properly-controlled AI applications optimise core-financial workflows, mitigate subjective human-judgement bias, reduce operational-error probability, cut redundant operating costs, improve corporate-financial-operation efficiency and risk-resistance capacity and facilitate high-quality digital-transformation in corporate finance.

References

1. Hou, X. (2025). Research on the digital transformation of enterprise financial accounting in the context of artificial intelligence. China Zhenhua (Group) Science & Technology Co., Ltd. Online publication date: November 27, 2025. Subject areas: Economics and Management Science; Information Technology. Classification code: F275; TP18.
2. Chen, H. (2026). The transformation and future prospects of enterprise financial management driven by artificial intelligence. Shenzhen Zhongxingxin Cloud Services Co., Ltd. Online publication date: February 6, 2026. Subject areas: Economics and Management Science; Information Technology. Classification code: F275; TP18.
3. Chen L. Governance Challenges of Generative-AI Applications in Corporate Financial Reporting[J]. Chinese Journal of Management Science, 2025,33(02):18-29.
4. Ye Q H, Huang S Z. Practical Exploration of Identifying Financial Fraud Enabled by AI Large-scale Models[J]. Chinese Certified Public Accountant, 2025(03):36-40.
5. Zhao J, Zhang S H, Xu Y D. AI-Driven Risk Reshaping: Corporate AI Adoption and Stock Price Crash Risk[J]. Journal of Central University of Finance & Economics, 2025(11): 91-106.

6. Dong, Y., Willcott, N., Yang, X., & Yang, Y. (2026). Growing up in the modern world: How does artificial intelligence enhance firm growth? Emerald Journal. DOI: 10.1108/MF-09-2024-0715.
7. Elouadi, S., & El Bouanani, H. (2026). The role of AI in economic and financial forecasting. In The Role of AI in Economic and Financial Forecasting (pp. 530). DOI: 10.4018/979-8-3373-3053-2. CLC: F224.
8. Li, X. (2025). Empirical study on the effectiveness of generative AI in financial risk management for small and medium enterprises. Scientific Journal of Economics and Management Research, *7*(9), 21-31. DOI: 10.54691/NRGJAS03.
9. Han, X., Wu, Y., & Li, X. (2026). Artificial intelligence adoption, dynamic capabilities, and firm risk-taking. Journal of International Financial Management & Accounting, *37*(2), 477-511. DOI: 10.1111/JIFM.70010.
10. Yin H, Yin X, Wen F. Artificial intelligence and climate risk: A double machine learning approach[J]. International Review of Financial Analysis, 2025,103:104169.
11. Crisanto J C, Mangano G. Operational Resilience for Artificial Intelligence in Financial Services[J]. Journal of Financial Regulation and Compliance, 2024,32(3):345-362.
12. Blum, A., & Raviv, A. (2026). The financial crisis, Basel III, and large banks' financial reports: a topic modeling approach. Finance Research Letters, 103, 109714. https://doi.org/10.1016/j.frl.2026.109714.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

