

# Research on the Optimization Path of Internal Control of Listed Technology Companies Enterprises Driven by Digital-Realistic Integration

Mingxi Han<sup>1</sup>, Yu Xing<sup>2</sup>, Ruowen Yi<sup>2</sup>

1. School of Finance, Dongbei University of Finance and Economics, Dalian 116025, China;

2. Jiangxi Institute of Talent and Industry Integration Development, East China Jiaotong University, Nanchang 330013, China

---

**Abstract:** Digital-real integration reconfigures the logic of enterprise operation through digital technology, which puts forward the demand for adaptive change in the internal control of listed technology companies. This paper adopts qualitative research methods, combines case studies and in-depth interviews, and systematically explores the optimization path of internal control of listed technology companies driven by digital-real integration. The study finds that although technology embedding can enhance the standardization of business processes, it is easy to cause system rigidity and inflexibility; data-driven enhances the risk warning ability but intensifies the challenges of data security and collaborative governance. Based on the three-dimensional perspective of "system-technology-organization," this paper proposes the optimization paths of dynamically adapted internal control framework design, application of intelligent tools, and cross-departmental collaborative mechanism construction and emphasizes the importance of composite talent cultivation and digital culture cultivation. The study's conclusions provide a theoretical basis and practical guidance for technology enterprises to realize risk-controlled digital transformation in digital-real integration.

**Keywords:** Digital-real integration; Technology enterprises; Internal control; Optimization path; Digital economy

---

## 1. Introduction

Digital-real integration is a new development paradigm for the deep integration of the digital economy and the real economy, which utilizes digital technology to reconfigure the rules of traditional industries and give rise to new business forms, models, and ecologies. Technological innovation has also increased the complexity of enterprise internal control, and the traditional internal control model often suffers from system rigidity and insufficient technological adaptation when dealing with new scenarios such as data security, process automation, and dynamic risk early warning. Therefore, optimizing the internal control system with the help of digital and real integration has become a key issue for technology enterprises to achieve high-quality development.

In digital transformation, internal control of technology enterprises faces multiple challenges. Data-driven enhancement of the risk warning ability exacerbated data security and collaborative governance challenges (Guo Yali, 2025). While the integration of digital technology has reconfigured the logic of enterprise operations and given rise to new business models, embedding technology can enhance the standardization of business processes. Still, it is prone to institutional rigidity and inflexibility (Zhang Fa-Xin, 2025), and the data-driven approach enhances the ability to warn of risks. Still, it also exacerbates the systemic risk due to the controversy over data sovereignty and the lack of collaborative governance mechanisms (Hu Cong-Jun, 2024).

This study is dedicated to analyzing the dynamic evolution of internal control of technology enterprises under the wave of digital integration. Following the logic of "theory construction - problem identification - path exploration," the study focuses on optimizing internal control in listed technology companies against the background of digital-real integration. Through multiple case studies and in-depth interviews, the study explores the core contradictions in internal control practices of technology enterprises in the context of digital-real integration. It analyzes the organizational roots and technological triggers of the problems. Finally, combining theoretical analysis and practical insights, a systematic optimization path is proposed, covering the application of technological tools, system flexibility design, and organizational capacity upgrading to ensure the adaptability and operability of the path.

## 2. Theoretical Basis and Literature Review

### 2.1 The concept of number-reality fusion and its role

Digital-real integration refers to the in-depth integration of digital technology and the real economy, which takes data as the key production factor and realizes enterprise model innovation, industrial integration and association, and intelligent decision-making through the support of connection, arithmetic power, and algorithm. In this process, data-driven can produce the “flywheel effect” and “snowball effect,” promote the key system links and data links in the industrial chain, and then reach the digital synergy and intelligent decision-making to improve enterprises’ production efficiency and market competitiveness.

### 2.2 Theoretical and practical research on internal control in listed technology companies

Internal control theory is highly critical in the field of business management. Its development history started with the internal control theory, which focused on business process design and reproduction at that time. Before the 1940s, the theory was in the embryonic stage, with the internal control theory as the core, and the American Institute of Certified Public Accountants (AICPA) defined internal control for the first time in 1936 and established the “four-functional statement,” which mainly prevented the financial fraud and preserved the assets. In 1949, AICPA formally defined internal control for the first time, which was divided into two parts: accounting control and management control. In 1988, the COSO Committee was established, and in 1992, COSO released the “Internal Control - Integration Framework,” which established the “Five Elements” model to guide theory and practice; in 2004, COSO released the “Enterprise Risk Management Framework,” which integrated risk management into internal control. In 2004, COSO issued the Enterprise Risk Management Framework, which integrates risk management into the internal control system. In 2002, the U.S. Sarbanes-Oxley Act pushed for the globalization of internal control compliance requirements. In 2013, COSO updated the internal control framework and strengthened the relevance of corporate governance. In 2017, COSO issued the Risk Management Framework, which realizes the integration of risk, strategy, and performance. In 2010, COSO issued the Risk Management Framework and the Risk Management Framework.

### 2.3 Theoretical Challenges of Digital-Realistic Integration for Internal Controls

Digital-real integration has reshaped the enterprise operation mode and management logic through the deep interaction between digital technology and the real economy, and it has also posed a multi-dimensional challenge to the traditional internal control theory. From the perspective of control objectives, traditional internal control theory takes risk prevention and control and compliance as the core objectives, emphasizing stable control through standardized processes. However, under the digital and real integration scenario, enterprises need to consider the dual objectives of innovation drive and technology risk prevention and control simultaneously.

Digital-real integration has posed subversive challenges to traditional internal control theories on five levels: goals, elements, boundaries, evaluation, and methodology. The essence of these challenges lies in the assumption of traditional theory premised on “stable environment - clear boundary - linear cause and effect” is fundamentally misaligned with the reality of “dynamic environment - ecological interconnection - non-linear interaction” of digital-realistic integration. To break through this dilemma, it is necessary to reconstruct the underlying logic of internal control theory and establish a new analytical framework of technological embeddedness, dynamic adaptability, and ecological synergy.

### 2.4 Literature review

As a paradigm for the deep integration of the digital economy and the real economy, the core of digital integration is reconfiguring the configuration of production factors, business processes, and business models through digital technology and promoting the digitalization, intelligence, and network upgrading of the real economy. In recent years, academics have systematically explored its connotation and mechanism from the perspectives of technology-driven data elements and industrial synergy.

Wenke et al. (2025) believe that the integration of digital and real technologies mainly optimizes the allocation of production factors, enhances the production efficiency and innovation ability of enterprises, strengthens market competitiveness, realizes the intelligence and automation of the production process, improves the production efficiency and product quality, reduces the cost of production, and improves the ability of market forecasting and demand management through the application of data elements. Zhang Bing et al. (2025) advocate that enterprises should strengthen the integration of digital and real technologies to enhance risk prevention and control capabilities through technological innovation and market expansion, and the government should encourage enterprises to strengthen the integration of digital and real technologies through policy support. Liu Huihui et al. (2025) emphasize that digital-real integration optimizes the allocation of capital resources, changes market demand and supply, and improves enterprises’ productivity and market competitiveness.

Hu Congjun (2024) emphasized that integrating data and reality promotes “system integration and innovation,” and listed technology companies should strengthen technological innovation and introduce advanced technology to improve internal control intelligence. Du Chuanzhong and Zhang Rong (2024) pointed out that perfecting the institutional mechanism of the data factor market can improve the effect

of enterprise internal control, and enterprises should improve the internal control system to ensure effective implementation. Wen Youyun (2024) shows that the cultivation of complex talents can improve the level of internal control, and enterprises should strengthen the cultivation of internal control talents to improve the awareness and ability of employees. Liu Yang (2024) pointed out that in the construction of digital industry clusters to promote the digital transformation of enterprises, enterprises should introduce a digital platform to realize the automation and intelligence of internal control processes. Chen Wenling et al. (2024) emphasize the important role of digital integration in enterprise internal control optimization, and enterprises should strengthen cooperation and communication with external institutions. Digital reality integration significantly improves enterprise risk prevention and control, audit compliance resource management, etc. Future research needs to explore its application and optimization path in enterprise internal control further.

### **3. Analysis of the current situation of internal control in listed technology companies**

#### **3.1 Characteristics of internal control in technology enterprises**

Due to their technology-intensive industry, the internal control system of listed technology companies shows obvious technology-oriented and dynamic adaptability characteristics. These characteristics not only shape the modernization of the enterprise's internal control but also deeply affect how the enterprise maintains the stability and security of its operations in the fast-changing technological environment.

Technological innovations and product updates are swift in the highly competitive technology industry. Taking Xiaopeng Automobile as an example, the company must frequently update and adjust its data security control strategy in developing its autonomous driving algorithms to cope with the rapid changes in regulations and constantly updated technical standards. However, traditional internal control manuals often fail to keep pace with technological iterations promptly due to their long revision cycles, resulting in a system that lags behind the needs of technological development. This lag may expose companies to compliance risks in innovation or even missed market opportunities. It highlights the vulnerability of internal control systems in a rapidly changing technological environment.

#### **3.2 Main Models of Current Internal Control Practices**

In the practice of internal control in the science and technology industry, enterprises have adopted diversified internal control models based on their technology application level and characteristics of the organizational structure. These models can be broadly categorized into the following three:

The centralized control model is the preferred choice of many head Internet companies. Under this model, the headquarters is responsible for uniformly formulating standardized internal control systems, which all branches must strictly follow. The advantage of this model is that it can ensure the compliance and consistency of the enterprise, especially in large-scale enterprises with massive scale and complex business, and can effectively maintain the stability and standardization of operations. However, the shortcomings of this model are also more apparent. As changes and adjustments to the system need to go through layers of approval, the process is more cumbersome, often resulting in the system's update speed lagging behind the speed of technological development.

Unlike centralized control models, distributed autonomy models are commonly found in blockchain startups. Such companies usually automate internal controls based on smart contracts and decentralized autonomous organizations. In this model, smart contracts automatically execute preset rules and processes, reducing the possibility of human intervention and increasing transparency and efficiency. However, this model is not without risk. Code vulnerabilities in smart contracts can lead to serious systemic problems.

On the other hand, hybrid models are standard among small and medium-sized SaaS providers. This model combines the empowerment of technology tools with manual intervention. For example, an organization may use financial software to handle basic financial processes but still rely on manual approvals for key decision-making aspects. The advantage of this model is that it can balance the cost and efficiency of technology application and manual management to a certain extent.

#### **3.3 Existing problems of internal control in technology enterprises**

In the highly competitive science and technology industry, to achieve effective internal control, enterprises often need to explore suitable internal control models in combination with their own technical level and organizational structure characteristics. However, current technology enterprises still face many core problems in internal control practice, which seriously limit the effectiveness of internal control.

The intelligent anti-fraud platform of Jingdong Digital Technology is a typical case. The platform handles massive amounts of transaction data daily and covers numerous business scenarios, significantly reducing the error rate of manual review. However, the internal control system requires a manual review of high-risk orders, resulting in only 40% of the system's effectiveness, highlighting the need for synergy between the technology and the system. Blockchain technology also plays an important role in enhancing audit transparency and reducing the risk of fraud by realizing chain-wide transparency of logistics, capital flow, and information flow through blockchain technology. Multi-chain isolated storage and cross-chain interaction models ensure the traceability of transaction data and effectively solve the credit transmission

problem in traditional finance.

Conflicts of authority between intelligent and manual systems have occurred occasionally, exposing possible adaptability problems in companies' technology applications. For example, Tesla's Autopilot-assisted driving system has led to several traffic accidents due to the conflict between the automatic execution logic and manual safety protocols. An investigation by the U.S. National Transportation Safety Board showed that Tesla Autopilot did not send out danger signals in time during the accident, while the driver did not maintain the takeover state due to over-reliance on the system. The ultimate responsibility attribution was ambiguous, highlighting the technological conflict between the rules and the artificial division of responsibility.<sup>110</sup> In addition, a blockchain supply chain finance platform was disconnected from business scenarios due to the automatic payment clause of the smart contract, which did not take into account the demand for market fluctuations and ultimately triggered supply chain disputes, forcing the enterprise to expend resources to reconstruct the logic of the contract.

In addition, the risk of a disconnect between technological publicity and institutional constraints should not be underestimated. For example, Tesla has over-advertised Autopilot as an "autopilot" function, making users mistakenly believe it can be completely detached from supervision. However, the system only has an L2 level of assisted driving.<sup>2022</sup> The court sentenced a car owner in Shenzhen for the crime of a traffic accident because of a series of rear-end collisions triggered by sleeping while using the assisted driving system, and the company faced legal liabilities due to misleading publicity. Misleading publicity faced legal recourse. Similar problems also appeared in the field of e-commerce; a business travel platform claimed "intelligent pricing," but in fact, the use of algorithms to implement big data on the old users "killed" consumers due to a price fraud lawsuit, the platform was ultimately sentenced to "a refund of one to compensate for three." The platform was eventually awarded "one refund and three compensations."

### 3.4 Differences in Industry Practices

The practice level of internal control of listed technology companies varies significantly according to enterprise scale and resource endowment, which is characterized by three levels of differentiation, namely, "leading technology but lagging system" for head enterprises, "efficiency bottleneck caused by fragmented application" for small and medium-sized enterprises, and "efficiency priority hiding compliance risks" for startup enterprises. The three levels of differentiation are characterized by "efficiency priority and hidden compliance problems."

The level of internal control practices in S&T firms shows significant differences depending on firm size and resource endowment.

Head enterprises invest heavily in intelligent internal control tools like AI wind control platforms and blockchain auditing systems. However, the system is not flexible enough, and the contradiction between technology application and system suitability is prominent. For example, the intelligent anti-fraud platform of Jingdong Digital Science handles hundreds of billions of transaction data daily, covering more than 600 business scenarios. However, in the early days, due to the system's requirement that all high-risk orders must be manually reviewed, the system's actual interception efficiency only reached 40%. In a promotion in 2022, the platform detected 150,000 suspicious transactions. However, due to the lagging speed of manual review, 32,000 fraudulent orders still completed the payment, with direct losses exceeding 20 million yuan. The conflict between the efficiency of technological tools and the long cycle of system revisions and redundant approvals inhibits the efficiency of innovation.

Limited by capital and talent, SMEs often adopt "patchwork" internal control, relying on open-source financial software to manage basic processes and outsourcing technical compliance teams to handle complex issues, resulting in a loose internal control system. For example, Tianyi Cloud Technology Co., Ltd. incurred a quarterly loss of RMB 200 million in the "Guangdong Enterprise Cloud" project due to the data silos between the financial system and the R&D system and the failure to correlate the server expansion and budget warning. In addition, 72% of SMEs have only automated less than 30% of their processes, resulting in limited efficiency gains.

In order to pursue speedy development, startups often "minimize internal control" at the cost of "minimizing internal control," skipping the data privacy impact assessment and launching new products directly, and dispersing the responsibility of internal control to non-professionals. For example, Editas Medicine (a gene-editing startup) suffered a permanent loss of core experimental data after an AWS server failure because it had not established a backup mechanism for R&D data, which directly led to the failure of its Series A financing and an 80% reduction in its valuation. Similar problems also appeared in the early stages of Wildberries; its AI anti-fraud system, due to the geographical deviation of the training data, mistakenly labeled the regular orders of Southeast Asian users as "high-risk," resulting in order cancellation rate of up to 25%, user turnover of more than 30%.

## 4. The mechanism of the influence of digital-real integration on the internal control of listed technology companies

### 4.1 Technology Embedding: Reconfiguring Internal Control Processes and Rules

Technology companies have significantly improved the efficiency and accuracy of their internal controls by introducing advanced tech-

nology tools. Lenovo Group shifted the internal audit process of employee reimbursement from manual operation to automated processing by deploying robotic process automation technology. The RPA robot combines OCR and intelligent dialog technology to automatically complete the download of electronic invoices, verification, and report generation, which saves about 1,500 hours of workforce costs per year, shortens the internal audit cycle by 87%, and achieves 100% data accuracy. In terms of blockchain application, the supply chain finance platform of Jingbei is based on FISCO BCOS blockchain technology, which realizes the traceability of the whole chain of transaction data and the automatic execution of smart contracts. The automatic payment instruction is triggered after the delivery of goods, shortening the time-consuming traditional paper-based process from weeks to hours while ensuring that the data cannot be tampered with, enhancing the transparency of the supply chain and the reliability of auditing.

In internal control, technology enterprises must skillfully balance technological innovation, risk prevention, and control according to their scale and characteristics. Leading companies are technologically advanced but often bound by traditional systems, so they should strive to break the system's rigidity and establish a more flexible internal control framework so that innovation and risk control can work together. On the other hand, SMEs are constrained by resources and fragmented internal control systems and urgently need to integrate fragmented systems, simplify processes, and enhance management effectiveness. In their pursuit of rapid development, startups often neglect compliance. They must balance efficiency and compliance to maintain innovation and market sensitivity while avoiding potential risks to ensure sustainable development.

#### **4.2 Data-driven risk management effects under digital-reality integration**

Data-driven has become the core means of risk management for technology enterprises. Its powerful real-time monitoring technology can accurately capture abnormal signals in the business process, dynamically adjust the risk assessment rules through in-depth analysis of user behavioral data, and, combined with machine learning models, thus significantly improve the enterprise's ability to identify risks. Suppose the enterprise's internal risk management process cannot keep up with the speed of technology detection, even if abnormal transactions are accurately identified. In that case, delays in the manual review process may result in the final payment of some fraudulent orders, thus bringing substantial economic losses to the enterprise.

As organizations' dependence on data-driven growth continues to grow, the potential harm caused by data security risks has been amplified accordingly. This highlights the importance of implementing complete life cycle data security management. Enterprises should focus on every aspect of data, from collection, storage, and processing to transmission, to ensure data security at all stages. To this end, enterprises must combine encryption technology and dynamic desensitization mechanisms to effectively reduce the systemic risks that may arise from data leakage. For example, advanced encryption standards can be used to encrypt sensitive data, and dynamic desensitization technology can be used to remove sensitive information in real-time when sharing data to protect the core data assets of enterprises.

Although data-driven risk management tools provide powerful and intelligent support for the internal control of technology enterprises, they may also become the source of new types of risks due to data security and governance issues if not handled properly. Therefore, enterprises need to make concerted efforts at the technical, institutional, and organizational levels to address the opportunities and challenges brought by data-driven jointly. At the technical level, enterprises should continue to strengthen encryption technology and algorithm transparency to improve data processing efficiency; at the institutional level, they should clarify data sovereignty through legal contracts and formulate clear data management policies; and at the organizational level, they need to build efficient cross-sectoral collaboration mechanisms to break down data silos and promote information flow.

#### **4.3 Organizational synergy and ecological risk management in digital-real integration**

In digital and real integration, enterprises need to break down traditional departmental barriers and promote the in-depth integration of finance, technology, and business departments to meet new development needs. This cross-departmental collaboration can effectively bridge the data silos and improve the global nature and agility of internal control decisions. By integrating production planning, equipment management, quality management, and other links, enterprises can build an intelligent decision-making platform with cross-departmental collaboration, thus realizing efficient resource integration and improved decision-making efficiency.

Organizations face many challenges in driving departmental integration. Different departments have significant differences in workflows, terminology, and technology tools, which can lead to communication barriers and inefficient collaboration. To overcome these barriers, companies must establish standardized workflows and information-sharing platforms to ensure smooth information exchange and collaboration across departments. At the same time, cross-departmental training and seminars can be conducted to promote mutual understanding and skill-sharing among personnel from different departments and enhance teamwork.

In addition, the risk boundary of enterprises under the digital-real integration extends to the supply chain and partners, and technical vul-

nerabilities may trigger a chain reaction through the digital link. In the face of this ecological risk, enterprises need to join hands with partners to formulate unified security standards and establish a real-time notification mechanism for vulnerabilities to block the risk conduction chain and safeguard the stability and security of the entire ecosystem. Enterprises should strengthen close cooperation with suppliers, customers, and other partners to build a safe and reliable digital ecosystem jointly.

## **5. Optimization Path and Countermeasure Suggestions**

### **5.1 Constructing a dynamic adaptation framework for internal control in listed technology companies**

Technology enterprises need to build a dynamically adapted internal control framework to break the rigidity and lag of traditional systems. Under the dynamic digital and real integration environment, enterprises should design a flexible system so that the internal control system can be adjusted in time with technology iteration and market changes.

The core of system optimization is to break the shackles of "static compliance" and achieve a dynamic balance between technology iteration and risk prevention and control through flexible design and agile revision mechanisms. Based on the thesis case, the dynamic adaptation of the internal control framework can significantly shorten the technology implementation cycle and avoid systemic risks in ecological collaboration through contractual governance. In the future, an AI-driven system self-optimization model can be further explored. However, it must strictly rely on the existing practice foundation to avoid detaching from the scene.

Intelligent tools provide strong support for the risk prevention and control of technology enterprises. Technological means such as AI risk monitoring, blockchain auditing, and big data governance improve the accuracy of risk identification and enhance the efficiency and reliability of internal control. The application of blockchain technology ensures the traceability of the whole auditing process, and its non-tampering characteristics provide a solid foundation of trust for enterprises. Meanwhile, through big data governance tools, enterprises can integrate decentralized systems and break down data silos. The key to technology integration lies in the deep embedding of intelligent tools into the business processes of enterprises, forming an organic integration of technology and business. This helps improve the enterprise's risk prevention and control capabilities and promotes the enterprise's digital transformation process.

Organizational change is an important means to meet the challenges of digital and real integration. Technology enterprises should promote cross-departmental collaboration, integrate the resources and processes of finance, technology, and business departments, and form a close cooperation mechanism. Information sharing and coordinated actions are promoted through the establishment of cross-departmental communication platforms and collaborative work processes to enhance the global nature and agility of internal control decisions. On this basis, build an ecological joint defense system to strengthen risk co-management with suppliers, customers, and other partners. We work with partners to formulate unified security standards and risk response strategies, establish real-time information sharing and vulnerability notification mechanisms, block the transmission of risks in the ecosystem promptly, and safeguard the stability and security of the entire business ecosystem.

Talent is the fundamental guarantee of internal control optimization. listed technology companies should cultivate a team of composite talents with dual knowledge of technology and management. By developing talent training programs and cross-departmental training, employees can adapt to the diversified job requirements under the integration of digital and real. At the same time, cultivate a digital culture within the enterprise to enhance employees' acceptance and application of digital tools and technologies. Through the organization of training, practical exercises, and cultural exchanges, digital thinking is deeply rooted in people's hearts and minds, providing a solid cultural foundation for the enterprise's digital transformation and internal control optimization.

### **5.2 Implementation Strategies for Internal Control Optimization in Technology Enterprises**

At the enterprise level, technology enterprises should take measures to optimize internal control. One is establishing a flexible internal control framework, reserving space to adapt to technological upgrades, simplifying the approval process, and accelerating innovation. The second is to promote the application of intelligent tools, integrate AI, blockchain, and other technologies to enhance the effectiveness of risk prevention and control, integrate data systems, break down information silos, and realize data sharing and collaboration. Third, strengthen cross-sectoral and external cooperation, build an ecological joint defense system, and ensure data security and risk co-management. Fourthly, we focus on talent training and digital culture construction to enhance employees' professionalism and digital thinking and provide a talent guarantee for internal control optimization.

The policy level should strongly support the optimization of internal control of technology enterprises. The government must improve data governance laws and regulations, provide compliance guidelines for cross-border data flows, etc., and create a favorable development environment. It should formulate industry standards and norms to improve enterprises' internal control level. At the same time, the government should promote school-enterprise cooperation to cultivate composite talents and meet the needs of enterprises for diversified talents. In addition,

tion, it should support enterprises in participating in international exchanges to help technology enterprises enhance their competitiveness in the international market.

At the industry level, internal control standards for digital-real integration should be actively established, successful experiences and technology applications should be promoted, and the overall level of development should be upgraded. Industry associations and other organizations should build experience-sharing platforms and promote exchanges and cooperation among enterprises. Training and seminar activities should be organized to disseminate advanced concepts and technology application cases. At the same time, it encourages enterprises to export their successful experiences, drive the digital transformation of small and medium-sized enterprises, and enhance the industry's overall competitiveness.

## 6. Conclusions and recommendations

This study systematically explores the dynamic evolution law and optimization path of the internal control of listed technology companies against the background of digital-realistic fusion. It is found that while the deep embedding of artificial intelligence, blockchain, and other technologies significantly improves the standardization of business processes, it also triggers contradictions such as system rigidity and algorithmic non-interpretability. For example, the high efficiency of technical tools requires rapid iteration. However, the traditional internal control system is challenging to adapt to the dynamic needs due to redundant approval levels and long revision cycles, resulting in a disconnect between the application of technology and the system's flexibility. In addition, the "black box" nature of the algorithm makes it difficult to attribute internal control failures (e.g., AI model decision logic is not traceable), which exacerbates the complexity of technology governance. The essence of this contradiction lies in the conflict between the efficiency improvement driven by technological innovation and the static compliance logic of traditional institutional design, and there is an urgent need to realize a balance between the two through a dynamic adaptation mechanism.

---

## References

- [1] Wen, K., & Li, C. H. (2025). Research on the impact of digital and real technology integration on the new quality productivity of enterprises. *Research Management*, 1-12.
- [2] Zhang, B., Zhang, L. W., & Zhou, H. H. (2025). Research on the impact of technological integration of digital and real industries on the stability of the global value chain of Chinese enterprises. *International Economic and Trade Exploration*, 1-18.
- [3] Shi, Y. T., Wang, X. D., & Zhou, S. T. (2025). Research on the employment effect of the integration and development of digital and real economies. *Journal of Beijing Institute of Technology (Social Science Edition)*, 25(01), 36-55.
- [4] Shi, B., & Hu, X. J. (2024). Mechanism Analysis and Realization Path of New Quality Productivity to Promote the Deep Integration of Digital and Realities. *Research on Socialism with Chinese Characteristics*, (06), 19-29.
- [5] Zhu, X. J., Wang, Y. X., & Wang, C. W. (2024). Re - measurement of the integration of China's digital and real economies - new findings from the depth of integration. *Journal of Guizhou University of Finance and Economics*, 1-13.
- [6] Chi, L. L., & Guo, F. (2024). Research on the impact of enterprise digital transformation on ESG performance. *Statistics and Decision Making*, 40(23), 173-177.
- [7] Zhang, S. H., Mu, X., Chen, X., & Li, M. L. (2024). Research on integrating digital economy and the real economy in China: a social reproduction process perspective. *China Soft Science*, (11), 35-45.
- [8] Yang, D. L., & Ding, C. X. (2024). Digital - real integration empowers high - quality economic development: factor - and technology - based integration. *Business Research*, (06), 77-90.
- [9] Du, C. Z., & Zhang, R. (2024). Research on sound institutional mechanisms to promote the deep integration of numbers and realities. *Research on Financial Issues*, (12), 16-27.
- [10] Liu, H. H., & Gao, J. Y. (n.d.). Multiple Advantages, Dynamic Analysis and Layout Improvement of New Quality Productivity by Digital and Real Integration. *Contemporary Economic Management*, 1-15.