Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 21, No. 3, 2026

Optimization path of network security governance system under the background of digital transformation

Cezhong Deng

Supervision & Test Station for Electronic Product of Sichuan Province, Chengdu, Sichuan, China

Abstract: Digital transformation not only releases the efficiency dividend of enterprises, but also significantly expands the network attack surface, which makes the traditional network security governance model face severe challenges. This paper systematically analyzes the four core pain points in the current governance system and the dilemma of governance logic reconstruction in zero trust transformation. Through the comparative study of mainstream governance paradigms such as NIST CSF 2.0, ISO 27001:2022 and zero trust architecture, this paper proposes a three-tier collaborative governance model covering strategic layer, operational layer and technical layer, emphasizing the horizontal integration of business-security-compliance. An empirical study of Group A shows that the model can shorten the decision-making period of cross-departmental security policy by 71.9%, reduce the time-consuming of new business security assessment by 84.9%, reduce the cost of multi-jurisdiction compliance integration by 50%, and reduce the response time of unauthorized access incident detection by 91.3%. The research provides a theoretical framework and practical path for the optimization of network security governance of digital transformation enterprises.

Keywords: Digital transformation; Network security governance; Collaborative governance model; Zero trust architecture; Compliance integration.

1. Introduction

Digital transformation has become the core strategy for global enterprises to maintain their competitiveness. Transformation not only releases the efficiency dividend, but also significantly expands the network attack surface of the organization. The traditional network security governance model has been difficult to match the current evolution speed of digital services. In this context, the importance of network security governance has been promoted to an unprecedented height. Governance is no longer just the responsibility of the technical department, but a systematic project involving strategic decision-making, organizational structure, compliance management and risk culture. The rise of zero trust architecture has further promoted the paradigm shift of governance logic from "border protection" to "continuous verification".

Most governance frameworks are still designed on the premise of traditional IT architecture, and their applicability is significantly reduced when faced with new infrastructure such as hybrid cloud, multi-tenant and micro-service [1]. The problem of governance fragmentation within the organization is prominent, and there is a lack of effective coordination mechanism among security teams, IT operation teams and business departments, which leads to the disconnection between security policies and business objectives [2]. The global compliance environment is becoming increasingly complex, enterprises need to meet multiple requirements of relevant laws and regulations, and compliance costs continue to rise, while the governance system does not provide an efficient integration path.

Through the systematic comparative analysis of mainstream governance paradigms such as NIST CSF 2.0, ISO 27001:2022 and zero trust architecture, this paper identifies four key challenges of the current governance system, and proposes a three-tier collaborative governance model, which covers the strategic layer, the operational layer and the technical layer, and emphasizes the integration of horizontal business, security and compliance. The model aims to provide a feasible governance optimization path for enterprises undergoing or planning digital transformation.

2. Challenges of current governance

2.1. The adaptability between traditional governance framework and new infrastructure is insufficient

At the beginning of design, the existing mainstream governance framework is mainly oriented to the relatively closed traditional IT architecture. With the wide adoption of hybrid cloud, multi-tenant environment, micro-service architecture and containerization technology, the IT boundary of enterprises is increasingly blurred, and the asset distribution is highly dynamic [3]. The traditional framework relies on static asset list, fixed network boundary and centralized management and control logic, which is difficult to effectively cover the scenarios of flexible scaling, cross-domain collaboration and continuous delivery in the cloud native environment [4]. This lack of adaptability leads to a blind spot in the actual implementation of governance strategies, and it is difficult to unify the safety baseline, thus forming a governance vacuum of "institutional existence and failure in implementation".

2.2. Fragmentation of internal governance and lack of coordination mechanism in organizations

Effective implementation of network security governance requires deep collaboration among security teams, IT operation teams and business departments [5]. At present, there are obvious "governance islands" in most organizations: the security department is often regarded as the undertaker of compliance costs rather than the enabler of business value;

Business departments often regard security review as a process obstacle when rapidly advancing digital projects [6]; The IT operation and maintenance team is faced with the continuous tension between the landing of security policies and the guarantee of system availability. This fragmentation is not only reflected in the organizational structure and division of responsibilities, but also in the deep mechanisms such as goal setting, performance appraisal and resource allocation. The lack of effective inter-departmental coordination mechanism leads to the serious disconnection between security policies and business objectives, and it is difficult for governance measures to be integrated into the whole life cycle of business processes.

2.3. Complexity of global compliance environment and lack of integration path

Digital transformation has made data flows of enterprises cross geographical boundaries, facing compliance pressures from multiple jurisdictions and standards. Regulatory frameworks represented by the EU General Data Protection Regulation (GDPR), the US California Consumer Privacy Act (CCPA), and Chinas Data Security Law and Personal Information Protection Law propose differentiated and sometimes conflicting requirements in areas such as cross-border data transfer, localized storage, and privacy-by-design [7-8]. In order to meet the compliance requirements, enterprises often need to build multiple sets of compliance systems in parallel, which leads to the continuous increase of compliance costs. More crucially, the existing governance system lacks the methodology of integrating scattered compliance requirements into a unified governance language, and compliance work stays in the passive mode of "item by item", which is difficult to transform into systematic governance capacity improvement.

2.4. Dilemma of reconstruction of governance logic in zero trust transformation

The rise of zero-trust architecture marks the fundamental change of network security paradigm from "border protection" to "continuous verification" [9]. This change puts forward new requirements for the governance system, and the governance object changes from static network boundary to dynamic identity and access behavior; The governance logic has changed from "once authentication and long-term access" to "never trust and always verify"; Governance responsibility has shifted from being exclusive to the security team to being embedded in every business interaction. Most organizations still follow the traditional governance thinking and organizational model when promoting zero trust transformation, which leads to the mismatch between technology architecture and governance mechanism. Specifically, the identity governance system has not yet established a unified standard, the fine-grained access control strategy lacks business context support, and the continuous monitoring and dynamic response mechanism is difficult to connect with the existing IT operation and maintenance process. This reconstruction dilemma makes it difficult to transform the zero-trust technology investment into the expected governance efficiency.

3. Three-tier collaborative governance model

As shown in Figure 1, this model is an optimization framework of network security governance for digital transformation scenarios, focusing on solving four core pain points: mismatch between traditional governance and new infrastructure, lack of inter-departmental collaboration, difficulty in compliance integration, and logical mismatch of zero-trust transformation, and constructing a collaborative governance system with vertical integration of strategic layer, operational layer and technical layer and horizontal integration of business, security and compliance, so as to realize dynamic matching between security governance and digital business evolution rhythm. The core value of the model lies in jumping out of the perspective of single technology optimization, upgrading network security from "subsidiary responsibility of technology department" to a systematic project covering strategic decision-making, organizational coordination and technology landing, and providing enterprises with a landing governance optimization path.

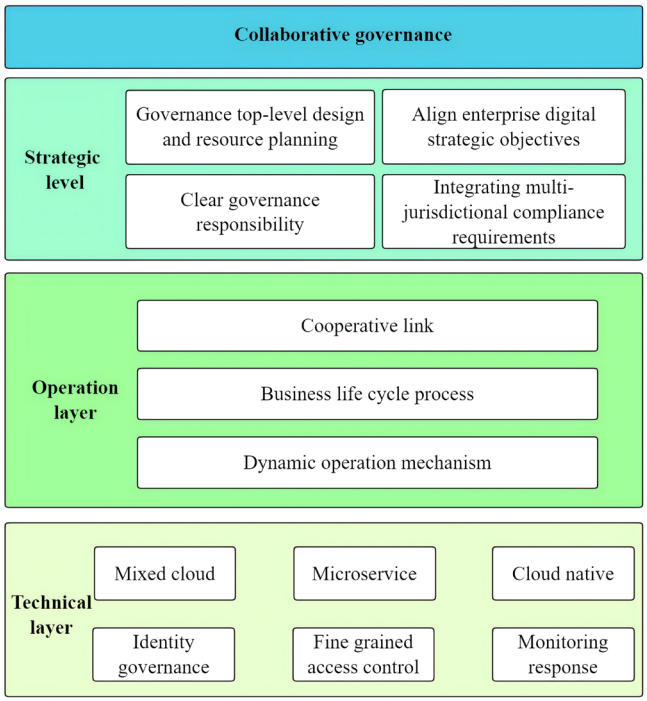

Figure 1. Three-tier collaborative governance model framework

(1) Strategic level

Manage the top-level design and resource planning, align the digital strategic objectives of enterprises, and clarify the governance responsibilities of the board of directors and senior management; Integrate compliance requirements of multiple jurisdictions, build a unified governance language and risk preference framework, and solve the problem of compliance fragmentation and governance islands.

(2) Operation layer

Cross-departmental process connection and mechanism landing, open up security, IT operation and maintenance, business department collaboration links, and embed security requirements into business life cycle processes; Establish a dynamic operation mechanism that adapts to the zero-trust paradigm and balance the requirements of security management and control and business agility.

(3) Technical layer

New infrastructure governance tools support, adapt to hybrid cloud, micro-service, cloud native and other technical architectures to replace the traditional static boundary control logic; Provide a technical base for identity governance, fine-

grained access control and continuous monitoring response for zero trust landing, and eliminate the blind area of governance coverage.

4. Case discussion

In order to verify the effectiveness of the three-tier collaborative governance model proposed in this paper, this study selects Group A as a single case for lightweight empirical analysis. Group A is a multinational manufacturing enterprise with annual revenue exceeding RMB 20 billion, covering R&D, production, supply chain and global sales. After the implementation of "Digital 2025" strategy, its network security governance system has exposed some typical problems, such as deep binding with traditional IT architecture, conflict between security strategy and agile development process, and sharp increase in the cost of multinational compliance with GDPR, CCPA and Chinas network security laws. The case study period is 12 months (from January 2024 to December 2024), and the governance system is reconstructed by action research method based on the model proposed above, and the key performance indicators before and after optimization are compared.

In view of the present situation of Group A, the research team deployed a three-tier collaborative governance model in three stages. At the strategic level, the Board of Directors of the Group approved the establishment of the "Network Security and Digital Transformation Governance Committee", which included security governance in the annual strategic balanced scorecard. At the same time, based on the governance domain of NIST CSF 2.0, 269 control items of 7 global regulations are integrated to form a unified enterprise-level security risk preference statement. The operation layer reconstructs the collaborative process of "security-development-operation and maintenance-business". Replace static annual penetration test with continuous security verification mechanism integrated with CI/CD pipeline. Introduce the role of "risk liaison officer", which is the backbone of the business department and is responsible for transforming business requirements into safety control baselines. At the technical level, the intelligent factory, the cloudy platform and the overseas marketing portal in the three core business areas of Group A have fully implemented a zero-trust architecture. Key technical components include fine-grained access control based on identity, network micro-isolation, and persistent behavior analysis engine.

In order to objectively evaluate the effect of the model, the research team defined key indicators in four dimensions, and collected corresponding data before (in 2023) and after (in 2024) the implementation of the model. The results are summarized in Table 1 and Figure 2.

Table 1. Comparison of key performance indicators of network security governance in A Group

Dimension	Key indicators	Before implementation (2023)	After implementation (2024)	Rate of change	Remarks
Governance efficiency	Average decision-making period of cross-departmental security policy (days)	18.5	5.2	-71.9%	Due to the unified risk language at the strategic level
Operational efficiency	Time-consuming for safety assessment before new digital business goes online (hours)	76.0	11.5	-84.9%	Thanks to automated process embedding at the operational level
Compliance cost	Multi-method compliance integration cost (million yuan/year)	23.6	11.8	-50.0%	Eliminate duplicate audit through unified control framework
Risk exposure	Average detection/response time of unauthorized access events (hours)	48.0	4.2	-91.3%	Technical layer zero trust continuous verification ability support

Note: All data are annual statistics of audit report and safety operation platform, and the change rate is statistically significant by t test, $p<0.05$.

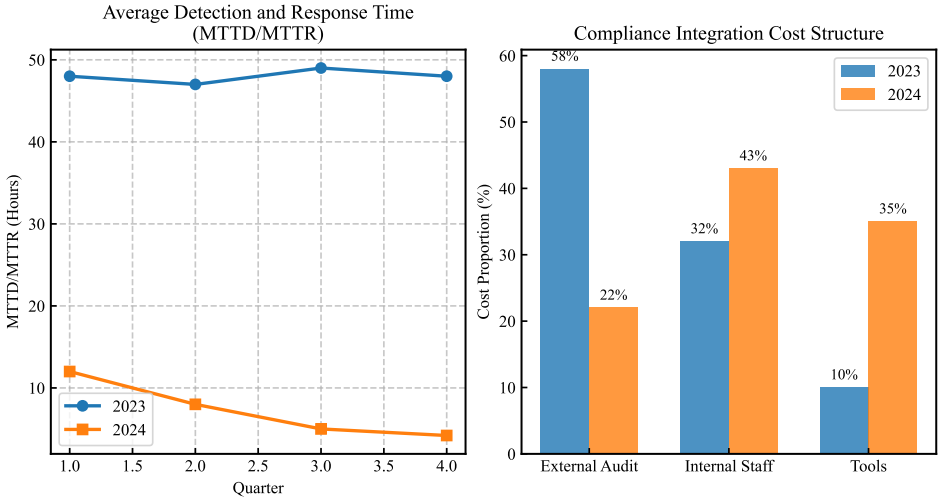

Figure 2. Security incident response and compliance integration cost trend

The practice of A Group shows that the three-tier collaborative governance model has effectively solved the

problem of disconnection between governance and business evolution in digital transformation. The integration of strategic level greatly reduces the friction of cross-departmental decision-making; The process reengineering of the operation layer makes security an organic part of the development assembly line, rather than "access control"; The zero trust in the technical layer directly translates into an order of magnitude improvement in risk response capability. It is particularly noteworthy that the cost of the master plan still decreases by 50% with the increase of tool input, which verifies the economic rationality of the model of "tools for efficiency".

However, this case has the following limitations: 1) As a single manufacturing case, the applicability of the model in different digital maturity industries such as finance and Internet needs to be further tested; 2) The observation period is only 12 months, which fails to evaluate the long-term toughness of the model; 3) The implementation of the model is highly dependent on high-level support, and it may face resistance in organizations lacking strategic commitment. Future research can adopt multi-case comparison or longitudinal follow-up design to enhance the external validity of the conclusion.

5. Conclusion

The three-tier collaborative governance model effectively realizes the dynamic matching between security governance and the evolution rhythm of digital services. By integrating multi-jurisdictional compliance requirements and risk preference framework, the strategic layer embeds security governance deeply into the strategic objectives of enterprises, which shortens the decision-making cycle of cross-departmental security policies; The operation layer reconstructs the collaborative process of "safety-development-operation and maintenance-business", and reduces the time-consuming of safety assessment before new business goes online through automation tools and risk liaison officer mechanism. After the introduction of zero trust technology, the cost of multi-method compliance integration of enterprises still decreased significantly, which verified the economic rationality of "tools for efficiency". The research breaks through the traditional technology-oriented thinking of network security governance and upgrades it to a systematic project covering strategic decision-making, organizational coordination and technology landing, which provides a practical path for the governance optimization of digital enterprises.

References

[1] Hammouri, M. M. G., Aljawarneh, M. N., Alazzam, F. A. F., & Alhyasat, W. (2026). Cybersecurity spending and IT capability development: The mediating role of IT governance effectiveness. EDPACS, 71(5), 82-92. https://doi.org/10.1080/07366981.2025.2564773

[2] Shoaib, M., & Alharbi, A. (2025). Convergence of cybersecurity governance, risk management and compliance (GRC) for IT and OT environments: Context of KSA. Journal of Computer and Communications, 13(12), 9-27. https://doi.org/10.4236/JCC.2025.1312002

[3] Bhandari, R. (2026). AI and cybersecurity: Opportunities, challenges, and governance. EDPACS, 71(4), 29-37. https://doi.org/10.1080/07366981.2025.2544363

[4] Falschau, A. R. K., Lamzihri, O., & Gagnon, S. (2026). Do governance determinants contribute to effective management of cybersecurity threats posed by misleading information? Evidence from Canadian organizations. International Journal of Accounting & Information Management, 34(2), 385-411. https://doi.org/10.1108/IJAIM-12-2024-0467

[5] Makhamreh, Z. H., Alhyasat, W., & Alhyasat, E. (2026). Global research frontiers in cyber security governance: A bibliometric and thematic analysis. EDPACS, 71(3), 51-65. https://doi.org/10.1080/07366981.2025.2536224

[6] Hossain, E., Bashir, M., Rashed, M. A. R., & Rahman, M. S. (2025). An integrated MIS–cybersecurity governance framework for risk-adaptive IT project management in critical infrastructure systems. Frontiers in Computer Science and Artificial Intelligence, 4(2), 13-25. https://doi.org/10.32996/FCSAI.2025.4.2.2

[7] Liu, C., & Babar, A. M. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management, 51(1), 62-92. https://doi.org/10.1177/03128962241293658

[8] Enam, M., Singh, N., & Das, N. (2026). Do cybersecurity policies influence the effectiveness of corporate governance on bank performance? Insights from Quad countries. Digital Policy, Regulation and Governance, 28(1), 92-110. https://doi.org/10.1108/DPRG-03-2024-0043

[9] Cai, Y. (2026). Research on the collaborative promotion path of network ideology security risk early warning and resilience governance in the new era. Journal of International Social Science, 3(4), 103-106. https://doi.org/10.62639/SSPJISS16.20260304