

Enterprise Supply Chain Risk Management Under Digital Transformation

YuXin Li. Min Lin

School of Economics and Management, Southwest Petroleum University, Chengdu 610500, Sichuan, China

How to cite this paper: Li, Y. X., & Lin, M. (2026). Enterprise Supply Chain Risk Management Under Digital Transformation. *Economics & Business Management*, 5(1), 123-133. ISSN Print: 3079-5214; ISSN Online: 3079-5222.

<https://doi.org/10.63313/EBM.9167>

Published: 2026-03-26

Copyright © 2026 by author(s) and Erytis Publishing Limited.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Abstract

Against the backdrop of a complex and volatile global economic environment, enterprise supply chains are exposed to multiple forms of disruption, including pandemics, geopolitical tensions, market instability, operational breakdowns, and digital vulnerabilities. Recent studies have shown that supply chain risk management has evolved from a narrow operational concern into a broader governance issue closely associated with resilience, adaptability, and long-term viability. At the same time, digital transformation has created new opportunities for improving visibility, coordination, forecasting, and decision-making, while also introducing risks related to cybersecurity, information fragmentation, and technological dependence. In this background, this paper proposes a conceptual framework for enterprise supply chain risk management by integrating recent literature on risk typology, resilience, and digital innovation. The study identifies four major categories of supply chain risk: supply risk, demand risk, operational risk, and information risk. It further argues that effective risk management should follow a dynamic process of risk identification, assessment, response, and monitoring. On this basis, the paper proposes a three-dimensional strategic framework composed of preventive strategies, responsive strategies, and innovation-oriented strategies under digital transformation. The findings suggest that enterprises can strengthen supply chain resilience not only through traditional measures such as supplier diversification, safety stock, and emergency planning, but also through digital technologies including big data analytics, the Internet of Things, artificial intelligence, blockchain, and digital twins. This study contributes to the understanding of supply chain risk governance in the digital era and provides practical implications for firms seeking to balance efficiency, resilience, and sustainability.

Keywords

Supply chain risk management; Digital transformation; Risk governance; Enterprise management; Innovation strategy

1. Introduction

Supply chains have become increasingly vulnerable in the contemporary business environment. Globalization, outsourcing, lean operations, and digital connectivity have significantly improved efficiency, but they have also made supply networks

more tightly coupled and more exposed to disruption. Recent shocks, especially the COVID-19 pandemic and post-pandemic turbulence, have highlighted the fragility of global supply systems and intensified academic attention to supply chain risk, resilience, and survivability (Ivanov & Das, 2020; Aljuneidi et al., 2023). These developments suggest that supply chain risk is no longer a peripheral operational issue, but a strategic concern with implications for continuity, performance, and competitive advantage.

Recent literature increasingly links supply chain risk management with resilience and long-term viability. Rather than merely responding to isolated disruption events, firms are now expected to build capabilities that allow them to prepare for, absorb, recover from, and adapt to severe shocks and prolonged uncertainty (Ivanov & Keskin, 2023). This shift reflects an important change in managerial thinking: the goal is no longer only to reduce disruption probability, but also to sustain enterprise functioning under complex and evolving external conditions.

At the same time, digital transformation has fundamentally reshaped supply chain management. Industry 4.0 technologies, enterprise digital transformation, artificial intelligence, data analytics, digital platforms, and connected devices have improved supply chain visibility, process integration, and real-time decision-making. However, these technologies have also introduced new risks related to data governance, information quality, cybersecurity, system reliability, and technology dependence (Spieske & Birkel, 2021). More recent empirical research also suggests that enterprise digital transformation is increasingly associated with supply chain resilience and performance under uncertainty (Zhao et al., 2023; Qi et al., 2024; Li et al., 2025; Zhang et al., 2025).

Although recent studies have provided substantial insight into supply chain risk management, resilience strategies, and digital technologies, there remains a need for a more integrated framework that connects risk categories, governance processes, and strategic responses. In particular, enterprises need a practical and theoretically grounded approach that clarifies what kinds of risks they face, how those risks should be managed, and how digital transformation can be leveraged to enhance resilience.

This paper addresses that need by developing a conceptual framework for enterprise supply chain risk management under digital transformation. Specifically, the study has three objectives. First, it identifies the major categories of enterprise supply chain risk. Second, it explains the principles and process of supply chain risk management. Third, it proposes a three-dimensional strategic framework of prevention, response, and innovation to support enterprise resilience in the digital era.

The remainder of the paper is organized as follows. Section 2 presents a conceptual overview of supply chain risk management. Section 3 analyzes the major types of enterprise supply chain risk and their influencing factors. Section 4 proposes a

strategic framework for enterprise supply chain risk management under digital transformation. Section 5 discusses the theoretical and managerial implications of the framework, and Section 6 concludes the paper.

2. Conceptual Overview of Supply Chain Risk Management

2.1. Definition of Supply Chain Risk Management

Although definitions vary across studies, recent reviews broadly agree that supply chain risk management involves the identification, assessment, mitigation, and monitoring of uncertainties that may negatively affect supply chain continuity and performance (Gurtu & Johnny, 2021). This view emphasizes that supply chain risk management is not limited to post-event response. Instead, it includes a structured set of managerial activities aimed at anticipating disruption, evaluating vulnerability, designing mitigation measures, and maintaining operational continuity under uncertainty.

Recent research has further expanded this understanding by connecting supply chain risk management with resilience and viability. Supply chain resilience research focuses on the ability of the supply chain to prepare for, respond to, and recover from disruptions, while viability-oriented research goes further by emphasizing the capacity of supply chains to survive and adapt under prolonged structural turbulence (Rahman et al., 2022). This development suggests that supply chain risk management should be treated as a dynamic governance capability rather than a static control mechanism.

Accordingly, this paper defines enterprise supply chain risk management as a dynamic and systemic governance process through which firms identify, assess, respond to, and continuously monitor internal and external risks across interconnected supply chain activities, with the aim of sustaining resilience and long-term viability. This definition reflects the increasing complexity of the external environment and the deeper interdependence created by digital transformation and networked supply systems (Ma et al., 2025).

2.2. Core Principles of Supply Chain Risk Management

Effective supply chain risk management is guided by several core principles.

The first is the preventive principle. Enterprises should not rely solely on reactive crisis management after disruptions occur. Instead, they should emphasize early warning, preparedness, and proactive governance. Recent resilience reviews show that preparedness-oriented actions such as visibility enhancement, risk sensing, strategic redundancy, and process redesign play a critical role in reducing vulnerability before shocks escalate (Rahman et al., 2022).

The second is the systematic principle. Supply chain risks are embedded in interconnected processes spanning procurement, production, inventory, logistics, information exchange, and customer fulfillment. Because risks may spread across

functions and organizations, effective risk governance must be cross-functional and system-wide rather than fragmented among isolated departments (Emrouznejad et al., 2023).

The third is the dynamic principle. The business environment is characterized by changing regulation, demand volatility, geopolitical instability, technology evolution, and sudden disruptions. This means that risk management strategies cannot remain fixed; they must be continuously updated in response to new threats and changing conditions (Parast, 2022; Ivanov & Keskin, 2023).

The fourth is the collaborative principle. Since supply chains involve multiple interdependent actors, risk governance requires cooperation among suppliers, manufacturers, logistics providers, distributors, and platform partners. Recent studies on digitalization and resilience indicate that coordination, information sharing, and network-level adaptation are increasingly important in modern supply chains (Li et al., 2025).

2.3. The Process of Supply Chain Risk Management

The literature generally conceptualizes supply chain risk management as a closed-loop process involving risk identification, risk assessment, risk response, and risk monitoring (Emrouznejad et al., 2023).

Risk identification is the starting point of the process. It aims to detect sources of uncertainty and disruption arising from internal operations, supply markets, demand conditions, logistics systems, digital infrastructure, and the broader macro-environment. Recent reviews suggest that risk identification should include both conventional operational risks and newly emerging digital and network-related risks (Aljuneidi et al., 2023; Culot et al., 2024).

Risk assessment evaluates the likelihood and potential impact of identified risks. It provides a basis for prioritization and resource allocation. Contemporary research increasingly treats assessment not only as probability-impact analysis, but also as a means of understanding interdependence, propagation, and survivability under different disruption scenarios (Liu et al., 2022).

Risk response refers to the design and implementation of mitigation, adaptation, and recovery actions. These may include supplier diversification, safety stock, flexible sourcing, alternative logistics arrangements, contractual protection, and rapid reconfiguration mechanisms. Recent literature suggests that response strategies are most effective when they integrate flexibility, redundancy, and digital support capabilities (Rahman et al., 2022).

Risk monitoring ensures continuous oversight and organizational learning. In the digital era, monitoring increasingly relies on integrated information systems, analytics, sensor-based tracking, and real-time dashboards that allow firms to detect anomalies early and update risk responses quickly (Qi et al., 2024; Zhang et al., 2025).

3. Major Types of Enterprise Supply Chain Risk and Their Influencing Factors

Recent literature reviews continue to show that enterprise supply chain risks can be grouped into several broad categories, among which supply risk, demand risk, operational risk, and information risk remain the most representative and analytically useful. These risks are interrelated and often propagate across the supply network rather than remaining confined to a single node.

3.1. Supply Risk

Supply risk refers to disruptions or uncertainties associated with upstream sourcing activities. It includes raw material shortages, supplier failure, delivery unreliability, quality instability, and vulnerability caused by concentrated procurement structures. In highly globalized and specialized supply networks, upstream disruption can quickly interrupt production continuity and increase total supply chain exposure (Gurtu & Johny, 2021).

Supply risk is driven by both internal and external factors. Internally, overdependence on limited suppliers, insufficient supplier evaluation, weak procurement strategy, and poor upstream visibility can magnify vulnerability. Externally, geopolitical conflict, trade restrictions, natural disasters, and sudden market fluctuations may all interrupt sourcing continuity. Recent post-pandemic research has reinforced the importance of diversification and preparedness in mitigating upstream fragility (Chauhan et al., 2023).

3.2. Demand Risk

Demand risk arises when actual market demand deviates significantly from forecasted demand. It may manifest as inventory accumulation, stockouts, unstable order flows, planning mismatch, or delayed response to changing customer preferences. In volatile markets, shortened product life cycles, competitive pressure, and demand uncertainty make accurate forecasting increasingly difficult (Guo et al., 2025).

The causes of demand risk also involve both internal and external dimensions. Internally, insufficient market intelligence, weak cross-functional coordination, and inadequate forecasting tools may distort demand planning. Externally, macroeconomic shifts, changes in customer behavior, and substitution driven by new technologies can alter consumption patterns rapidly. Under such conditions, demand risk often interacts with supply and inventory risk, thereby amplifying disruption throughout the supply chain network.

3.3. Operational Risk

Operational risk concerns disruptions within internal production, warehousing, transportation, and fulfillment processes. Typical examples include equipment

failure, production interruption, logistics delay, process bottlenecks, labor shortages, and quality defects. These risks directly affect the enterprise's ability to maintain continuity and meet customer requirements.

Recent resilience studies suggest that operational risk has become more visible under disruption conditions because firms often face simultaneous pressure on production capacity, labor availability, transportation reliability, and delivery performance (Parast, 2022). Internal causes include outdated equipment, insufficient maintenance, poor process design, and inadequate organizational flexibility. External causes include energy instability, labor market volatility, transport constraints, and supplier-related propagation effects. Since operational risk connects upstream and downstream activities, it often functions as a central transmission mechanism through which disruption spreads across the supply chain.

3.4. Information Risk

Information risk has become increasingly significant in digitally connected supply chains. It includes inaccurate or delayed information transmission, data fragmentation, cybersecurity threats, system downtime, platform failure, and excessive dependence on digital infrastructure. As enterprises adopt data-driven decision systems, artificial intelligence, the Internet of Things platforms, and cloud-based coordination tools, the reliability and security of information flows become critical to supply chain performance (Culot et al., 2024).

Information risk is shaped by both organizational and technological conditions. Internally, weak data governance, insufficient cybersecurity capability, low data quality, and fragmented information systems can reduce visibility and decision quality. Externally, cyber threats, platform dependence, regulatory pressure, and third-party technology vulnerability can expose enterprises to new forms of disruption. Recent digital transformation studies suggest that improved resilience depends not only on adopting digital tools, but also on ensuring their secure, coordinated, and strategically aligned use (Zhang et al., 2025).

4. A Three-Dimensional Strategic Framework for Enterprise Supply Chain Risk Management

To address the multidimensional nature of enterprise supply chain risk, this paper proposes a three-dimensional framework consisting of preventive strategies, responsive strategies, and innovation-oriented strategies. The logic of this framework is that resilience cannot be achieved through reactive action alone. Firms need to reduce the probability of disruption, improve their capability to absorb and recover from shocks, and continuously strengthen adaptability through digital and organizational innovation.

4.1. Preventive Strategies

Preventive strategies focus on reducing the likelihood of disruption before it occurs. One of the most important measures is supplier diversification. Multi-sourcing and balanced supply base design can reduce dependence on single suppliers and lower the risk of upstream interruption. Recent resilience reviews repeatedly identify supplier diversification, strategic redundancy, and structural flexibility as important preparedness-oriented mechanisms.

Another preventive strategy is the strengthening of visibility and early warning capability. By improving demand sensing, supplier monitoring, inventory transparency, and process traceability, enterprises can detect abnormalities earlier and respond before they escalate into severe disruptions. Recent digital resilience studies indicate that visibility is increasingly supported by data integration, platform connectivity, and enterprise digital transformation (Qi et al., 2024).

Preventive governance also requires process redesign and inventory preparation. Although lean management remains important for efficiency, recent work from the inventory management perspective suggests that stockpiling, capacity reservation, flexible contracts, and risk-sensitive inventory design remain central tools for resilience under uncertain supply and demand conditions (Guo et al., 2025). Therefore, prevention should be understood as a balance between efficiency and strategic preparedness rather than a purely cost-minimizing exercise.

4.2. Responsive Strategies

Responsive strategies focus on the enterprise's ability to absorb disruption, maintain continuity, and recover after shocks occur. Recent resilience literature highlights flexibility, response speed, recovery capability, and adaptive reconfiguration as critical dimensions of effective supply chain response.

One major responsive mechanism is operational flexibility, including the ability to switch suppliers, reallocate production, adjust logistics arrangements, and revise planning quickly. Such flexibility allows firms to limit disruption losses and preserve service continuity when normal operating conditions are interrupted.

A second mechanism is recovery capability, which involves contingency planning, emergency communication, crisis coordination, and restoration of disrupted flows. Recent studies suggest that enterprises should not only prepare for short-term interruption but also develop longer-term adaptation capacity under extraordinary scenarios (Ivanov & Keskin, 2023). This implies that response strategies should extend beyond isolated emergency action and include mechanisms for dynamic re-planning and network-level coordination.

A third mechanism is adaptive redundancy. While redundancy is often associated with inefficiency, recent resilience research shows that carefully designed redundancy in inventory, logistics options, and supply arrangements can serve as a crucial buffer against severe uncertainty (Guo et al., 2025). Thus, responsive capability depends on balancing flexibility, redundancy, and decision speed.

4.3. Innovation-Oriented Strategies Under Digital Transformation

The third dimension of the framework emphasizes innovation-oriented strategies enabled by digital transformation. Recent literature consistently shows that digital technologies can strengthen supply chain resilience by improving transparency, coordination, information processing, and dynamic capability.

First, artificial intelligence can support forecasting, planning, risk detection, and decision-making. Systematic reviews show that AI is increasingly applied in demand forecasting, procurement analysis, logistics optimization, and decision support, although scholars also caution that actual empirical validation remains important (Toorajipour et al., 2021).

Second, enterprise digital transformation can enhance resilience by integrating data, improving process visibility, and enabling faster cross-functional coordination. Recent empirical evidence suggests that digital transformation has a positive association with supply chain resilience and performance, especially when it improves information sharing and resource orchestration (Fan et al., 2025).

Third, Industry 4.0 technologies and connected systems such as IoT platforms, smart devices, and digital monitoring tools improve real-time visibility and facilitate earlier response to disruption signals. These technologies support more accurate tracking of flows, assets, and process conditions, thereby enhancing operational awareness and resilience (Spieske & Birkel, 2021).

Fourth, blockchain and advanced digital infrastructure may also contribute to resilience by improving traceability, verification, and trust across supply chain relationships. However, recent review work suggests that blockchain should be treated as a conditional enabler rather than a universal solution, because its resilience effects depend on context, implementation quality, and the specific type of disruption involved (Beck et al., 2023).

Overall, innovation-oriented strategies should not be seen as a replacement for traditional risk management. Instead, they should complement preventive and responsive measures by strengthening information quality, coordination speed, and adaptive decision-making. In this sense, digital transformation becomes a strategic capability that enables more intelligent and resilient supply chain governance.

5. Discussion

This paper suggests that recent supply chain risk management research has shifted from static classification toward a broader emphasis on resilience, viability, and digitally enabled adaptation. Recent reviews show that the field is moving beyond basic risk identification toward integrated discussions of network vulnerability, strategic preparedness, dynamic response, and long-term survivability. This shift is especially important in the post-pandemic environment, where disruption is no longer treated as exceptional but as a recurring feature of the business landscape.

From a theoretical perspective, the proposed framework contributes by integrating

risk categories, governance processes, and strategic responses into a coherent conceptual model. Rather than treating supply risk, operational risk, demand risk, and information risk as isolated phenomena, the framework emphasizes their interdependence and their connection to broader resilience-building capability. This is consistent with contemporary viability and contingency perspectives, which argue that enterprise performance under disruption depends on both structural preparedness and adaptive capability.

From a managerial perspective, the framework implies that enterprises should not rely solely on traditional mitigation measures such as safety stock or supplier substitution. While these remain important, firms increasingly need an integrated approach that combines preparedness, response capability, and digital innovation. Recent empirical studies indicate that digital transformation can improve supply chain resilience, but only when it is supported by appropriate organizational capability, information quality, and strategic coordination.

The discussion also highlights an important caution: digitalization does not automatically eliminate risk. Instead, it may shift risk from physical disruption toward information dependence, system complexity, and technological vulnerability. Therefore, enterprises should combine digital investment with governance mechanisms that ensure cybersecurity, data quality, interoperability, and organizational readiness.

This study is conceptual in nature and therefore has limitations. It does not include empirical testing, case-based validation, or industry comparison. Future research may test the proposed framework across sectors, explore how different digital technologies affect distinct categories of risk, and examine how resilience interacts with sustainability and network structure under long-term uncertainty.

6. Conclusion

In an era characterized by uncertainty, disruption, and digital transformation, enterprise supply chain risk management has become a strategic priority. Based on recent literature from 2020 to 2025, this paper has shown that enterprise supply chains face four major categories of risk: supply risk, demand risk, operational risk, and information risk. It has also argued that effective risk governance should be understood as a dynamic process of identification, assessment, response, and monitoring.

On this basis, the paper proposes a three-dimensional framework of prevention, response, and innovation. Preventive strategies reduce vulnerability through diversification, preparedness, and visibility improvement. Responsive strategies strengthen the ability of enterprises to absorb shocks, reconfigure operations, and recover from disruption. Innovation-oriented strategies enhance resilience by leveraging digital transformation, artificial intelligence, connected systems, blockchain, and data-driven coordination.

Overall, the study suggests that supply chain resilience is not produced by any single tool or isolated policy. Rather, it emerges from the integration of organizational design, strategic preparedness, adaptive response, and digitally enabled governance. This integrated perspective may provide useful guidance for both researchers and practitioners seeking to improve enterprise supply chain risk management in the digital era.

References

- [1] Aljuneidi, T., Bhat, S. A., & Boulaksil, Y. (2023). A comprehensive systematic review of the literature on the impact of the COVID-19 pandemic on supply chains. *Supply Chain Analytics*, 3, 100025.
- [2] Beck, J., Birkel, H., Spieske, A., & Gebhardt, M. (2023). Will the blockchain solve the supply chain resilience challenges? Insights from a systematic literature review. *Computers & Industrial Engineering*, 185, 109623.
- [3] Chauhan, C., Akram, M. U., Patky, J., & Chauhan, A. (2023). Mapping pathways for building resilient supply chains: A systematic literature review. *Journal of Cleaner Production*, 425, 138701.
- [4] Culot, G., Podrecca, M., & Nassimbeni, G. (2024). Artificial intelligence in supply chain management: A systematic literature review of empirical studies and research directions. *Computers in Industry*, 162, 104132.
- [5] Emrouznejad, A., Abbasi, S., & Sıcakyüz, Ç. (2023). Supply chain risk management: A content analysis-based review of existing and emerging topics. *Supply Chain Analytics*, 3, 100031.
- [6] Fan, L., He, J., Su, B., & Wang, C. (2025). Digital technology penetration and supply chain resilience improvement: Enterprise innovation strategies in the digital age. *International Review of Financial Analysis*, 104722.
- [7] Guo, Y., Liu, F., Song, J.-S., & Wang, S. (2025). Supply Chain Resilience: A Review from the Inventory Management Perspective. *Fundamental Research*, 5(2), 450-463.
- [8] Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. *Risks*, 9(1), 16.
- [9] Ivanov, D., & Das, A. (2020). Coronavirus (COVID-19/SARS-CoV-2) and supply chain resilience: A research note. *International Journal of Integrated Supply Management*, 13(1), 90–102.
- [10] Ivanov, D., & Keskin, B. B. (2023). Post-pandemic adaptation and development of supply chain viability theory. *Omega*, 116, 102806.
- [11] Li, P., Chen, Y., & Guo, X. (2025). Digital transformation and supply chain resilience. *International Review of Economics & Finance*, 104033.
- [12] Liu, M., Liu, Z., Chu, F., Dolgui, A., Chu, C., & Zheng, F. (2022). An optimization approach for multi-echelon supply chain viability with disruption risk minimization. *Omega*, 112, 102683.
- [13] Ma, C., Zhang, L., You, L., & Tian, W. (2025). A review of supply chain resilience: A network modeling perspective. *Applied Sciences*, 15(1), 265.
- [14] Parast, M. M. (2022). Toward a contingency perspective of organizational and supply chain resilience. *International Journal of Production Economics*, 250, 108667.
- [15] Qi, R., Ma, G., Liu, C., Zhang, Q., & Wang, Q. (2024). Enterprise digital transformation and supply chain resilience. *Finance Research Letters*, 66, 105564.
- [16] Rahman, T., Paul, S. K., Shukla, N., Agarwal, R., & Taghikhah, F. (2022). Supply chain resilience initiatives and strategies: A systematic review. *Computers & Industrial Engineering*, 170, 108317.
- [17] Spieske, A., & Birkel, H. (2021). Improving supply chain resilience through Industry 4.0:

A systematic literature review under the impressions of the COVID-19 pandemic. *Computers & Industrial Engineering*, 158, 107452.

- [18] Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. *Journal of Business Research*, 122, 502–517.
- [19] Zhang, J., Miao, X., & Shang, T. (2025). Impact mechanism of digital transformation on supply chain resilience. *Finance Research Letters*, 76, 106993.
- [20] Zhao, N., Hong, J., & Lau, K. H. (2023). Impact of supply chain digitalization on supply chain resilience and performance: A multi-mediation model. *International Journal of Production Economics*, 259, 108817.