

ASSESSING THE IMPACT OF ISO 28000:2022 SECURITY MANAGEMENT SYSTEMS ON SUPPLY CHAIN RESILIENCE AND RISK MITIGATION

OLATUNJI AKINYEYE, ABISOLUWA ABRAHAM ODUTOLA & DAMILOLA BADEJO
Texas A & M University- Kingsville

Abstract

This research examines the impact of ISO 28000:2022 Security Management Systems on supply chain resilience and risk mitigation. The study employs a qualitative approach, analyzing existing literature to assess the effectiveness of ISO 28000 in enhancing supply chain resilience, mitigating security risks, and identifying implementation challenges and success factors. Findings suggest that ISO 28000 plays a significant role in bolstering supply chain resilience by providing a structured framework for security management, promoting collaboration among supply chain partners, and facilitating continuous improvement. However, challenges such as resource constraints and organizational resistance to change exist. The study offers recommendations for organizations seeking to adopt ISO 28000 to improve supply chain security and resilience. Overall, the research contributes to the understanding of the mechanisms through which ISO 28000 influences supply chain resilience and highlights the importance of proactive security management in today's dynamic business environment.

Keywords: ISO 28000:2022, security management systems, supply chain resilience, risk mitigation.

1. Introduction

1.1 Background

The globalization of the economy has led to increasingly complex and interconnected supply chains, rendering them more susceptible to disruptions (Jüttner et al., 2003). These disruptions, stemming from diverse sources such as natural disasters, cyberattacks, theft, and political instability, underscore the critical need for organizations to fortify their supply chain resilience to ensure business continuity (Sodhi et al., 2018). In response to these challenges, standards such as ISO 28000:2022 have been developed, building upon previous versions to address evolving security concerns within the dynamic business landscape.

The ISO 28000:2022 standard was revised fifteen years after its initial publication to align with other ISO management system standards and increase clarity and consistency (Thijs Willaert 2022). This revision is significant as it sets the stage for research into its impact on supply chain resilience and risk mitigation. Building upon previous versions, ISO 28000:2022 incorporates contemporary best practices and requirements to tackle emerging security threats. By adhering to the principles outlined in this standard, organizations can strengthen their ability to identify, assess, and mitigate security risks across the entire supply chain, ultimately enhancing resilience and ensuring uninterrupted operations. Numerous organizations are facing an increasingly uncertain and volatile security landscape, prompting a critical shift in focus towards security concerns that directly impact their objectives. Implementing a structured security management approach can directly enhance an organization's business

capabilities, credibility, and resilience (PECB, 2023). This structured approach should encompass all activities, functions, and operations that influence the organization's security vulnerabilities, encompassing immediate threats, ongoing breaches, and associated security risks. The ISO 28000 standard leverages the Plan-Do-Check-Act (PDCA) model for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continuously improving the effectiveness of the organization's security management system (DNV, 2023). Supply chain resilience and risk mitigation are critical aspects of any organization's operations. With the increasing complexity of global supply chains, the need for effective security management systems has become more apparent. The ISO 28000:2022 standard aims to address this need by providing a framework for establishing, implementing, maintaining, and improving a security management system (ISO, 2022). However, the impact of the ISO 28000:2022 standard on supply chain resilience and risk mitigation is not well understood. There is a gap in the literature regarding the effectiveness of this standard in enhancing supply chain resilience and mitigating risks. This study aims to address this gap by assessing the impact of the ISO 28000:2022 standard on these aspects.

1.2 Statement of the Problem

Despite the increasing recognition of the importance of supply chain security and resilience, there remains a lack of comprehensive understanding regarding the effectiveness of ISO 28000:2022 in enhancing these crucial aspects. While the standard provides a structured framework for security management within supply chains, its practical impact on resilience and risk mitigation remains uncertain. This gap in understanding poses significant challenges for organizations seeking to strengthen their supply chain security measures and adapt to dynamic and evolving threats.

1.3 Objectives of the Study

The aim of this study is to investigate the impact of ISO 28000:2022 Security Management Systems on supply chain resilience and risk mitigation. The goal is to assess the effectiveness of ISO 28000:2022 in enhancing supply chain resilience and also to evaluate the role of ISO 28000:2022 in mitigating security risks within the supply chain.

2. Literature Review

2.1 Evolution of Supply Chain Management

Supply Chain Management (SCM) involves analyzing the intricate connections and relationships among various functions, processes, and stakeholders within a supply chain, with a focus on understanding how their interactions influence value creation and profit optimization (Ballou, 2007).

The evolution of supply chain management (SCM) spans over decades, reflecting the changing paradigms and priorities within the field. In its nascent stages during the early 20th century, SCM primarily focused on rudimentary logistics activities such as warehousing, transportation, and inventory management (Mentzer, J. T. et al, 2001). However, these activities were often disjointed and managed in isolation from each other. The Logistics Era, spanning from the 1950s to the 1970s, marked a significant shift towards a more integrated approach to physical distribution activities (Langley et al., 1982). During this period, the concept of logistics gained prominence, driving efforts to optimize transportation routes,

enhance warehouse efficiency, and minimize inventory levels. The subsequent Materials Management Era, extending from the 1970s to the 1980s, witnessed a growing emphasis on the upstream aspects of the supply chain, including procurement, materials planning, and supplier relationships (Monczka et al., 1998). This era also saw the widespread adoption of Just-in-Time (JIT) inventory management principles, aimed at streamlining operations and reducing waste. The advent of the Supply Chain Management (SCM) Era in the 1990s heralded a paradigm shift in how organizations approached their supply chain activities. With a focus on collaboration, information sharing, and risk management across the entire supply chain network, organizations began to view their suppliers and customers as integral partners in their operations (Mentzer et al., 2001). This era saw the emergence of supply chain integration as a core strategy for enhancing efficiency and responsiveness. Looking ahead, the future of SCM is poised for further transformation driven by advancements in technology. With the continued evolution of automation, artificial intelligence, and the Internet of Things (IoT), the future supply chain is expected to be characterized by real-time visibility, predictive analytics, and dynamic responsiveness (Gunasekaran et al., 2019). These technological advancements hold the potential to revolutionize supply chain operations, enabling organizations to anticipate and adapt to changes in demand and market conditions more effectively. Through each stage of its evolution, supply chain management has evolved to meet the changing needs and challenges of the business environment.

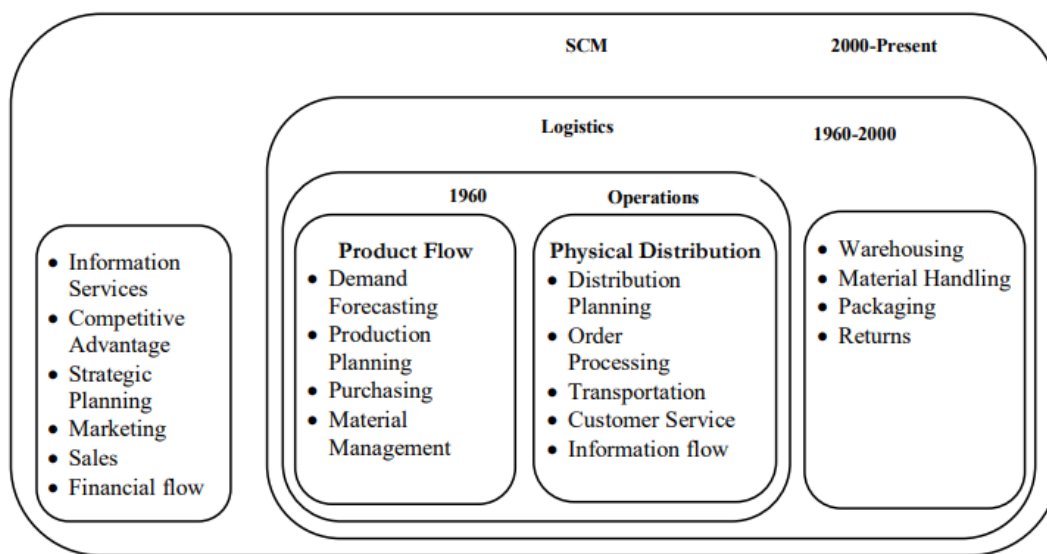


Fig 1: Evolution of SCM across the years

2.2 Supply Chain Security

The increasing complexity and interconnectedness of global supply chains have introduced new vulnerabilities. These vulnerabilities expose organizations to a range of security threats. Supply chains face a growing threat from cyberattacks, posing risks of operational disruptions, data breaches, and infrastructure compromise (PwC, 2023). Additionally, the proliferation of counterfeit goods and piracy poses challenges, including damage to brand reputation, revenue loss, and safety concerns for consumers (OECD, 2020). Instances of theft and diversion within the supply chain contribute to financial losses and product shortages, underscoring the need for vigilance (Bellantoni et al., 2020). Moreover, supply chains remain vulnerable to natural disasters and disruptions like political unrest, which can inflict severe

economic harm and impede operations (Jüttner et al., 2003). While Supply Chain Security (SCS) is widely acknowledged as critical, formal definitions of SCS remain sparse. In this study, SCS is defined as the implementation of policies, procedures, and technology to safeguard supply chain assets, including products, facilities, equipment, information, and personnel, from theft, damage, or terrorism. Additionally, it aims to prevent the introduction or unauthorized entry of contraband, individuals, or weapons of mass destruction into the supply chain (Closs and McGarrell, 2004, p. 8). This definition underscores the dual focus of SCS, which involves protecting against both outbound product breaches and inbound contraband entry, representing potential disruptions to the flow between organizations (Jüttner, 2005, p. 122).

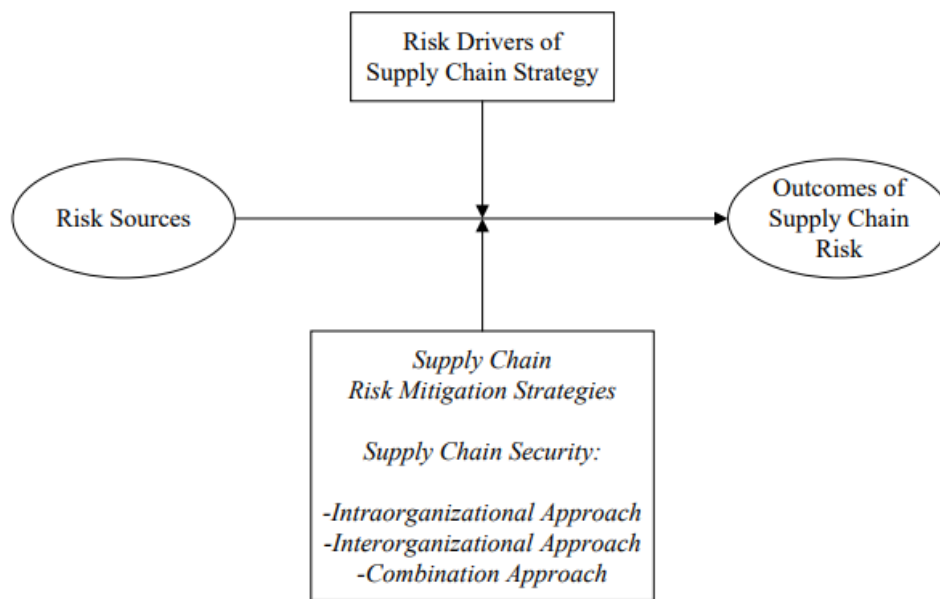


Figure 2: Updated model of supply chain risk management (: Jüttner et al., 2003)

2.3 Overview of ISO 28000 Standard

The ISO 28000 standard provides a comprehensive framework for implementing security management systems within the supply chain context. Developed by the International Organization for Standardization (ISO), ISO 28000 outlines requirements and best practices aimed at enhancing security measures and mitigating risks throughout the supply chain (ISO, 2022). This standard encompasses various aspects of supply chain security, including risk assessment, threat identification, and the establishment of security controls and procedures. The ISO 28000 series of standards focuses on Security Management Systems (SMS) specifically designed for the supply chain. The flagship standard, ISO 28000:2022, provides a framework for organizations to establish, implement, maintain, and continually improve their security posture across the entire supply chain (DNV, 2023). This standard goes beyond its original focus on physical security and encompasses a holistic approach to mitigating security risks throughout the supply chain network (International Organization for Standardization, 2022).



Fig 3: ISO 28000, Principles

2.4 Theoretical Framework

Organisational theories play a fundamental role in shaping the framework of supply chain management (SCM), providing essential foundations upon which SCM strategies are built. Extensive research has been conducted to explore these underlying theories (Ketchen Jr. and Giunipero, 2004; Ketchen and Hult, 2006), aiming to elucidate their significance in understanding the traditional viewpoints of SCM and its evolutionary trajectory over time. One such theory, the Resource-Based View (RBV), stands out as a dominant dimension in SCM. RBV emphasizes the strategic significance of possessing rare, valuable, and non-substitutable resources that confer competitive advantage (Barney, 1991).

The Knowledge-Based Theory sheds light on the coordination of supply chains, particularly in the absence of formal hierarchical structures. Unlike traditional organizational models reliant on hierarchies for coordination, supply chains often rely on knowledge to facilitate concerted actions. The accumulation and dissemination of critical knowledge within supply chains are essential for achieving coordinated operations (Grant, 1996).

2.4 Research Gaps

Research examining the relationship between ISO 28000 and supply chain resilience has made significant strides, While there is theoretical support for the potential impact of ISO 28000 on supply chain resilience, empirical evidence is still limited.

3.0 Methodology

3.1 Research Design

The research design involves a comprehensive review and synthesis of existing literature on ISO 28000 and supply chain resilience. This includes academic articles, industry reports, case studies, and other relevant sources. This approach is well-suited for exploring a relatively

under-researched phenomenon, like the impact of ISO 28000:2022 on supply chain resilience (Polit & Beck, 2014).

3.2 Data Collection

Data collection primarily involves gathering existing literature and studies related to ISO 28000 and supply chain resilience. Academic databases such as PubMed, Scopus, and Web of Science will be searched using relevant keywords and search terms, including "ISO 28000," "supply chain resilience," "security management systems," and variations thereof.

3.3 Data Trustworthiness and Rigor

To ensure the trustworthiness and rigor of the study, several strategies will be employed. These include triangulation of data sources to corroborate findings, member checking to validate interpretations with relevant stakeholders, and reflexivity to acknowledge and address potential biases in the research process (Creswell & Creswell, 2017).

3.4 Ethical Considerations

Ethical considerations will be paramount throughout the research process. All data will be obtained from publicly available sources, and proper attribution will be given to authors and sources. Confidentiality and anonymity will be maintained, and informed consent will not be required as the study involves analysis of existing literature rather than direct interaction with human participants.

4. Results

4.1 Effectiveness of ISO 28000:2022 in Enhancing Supply Chain Resilience

The assessment of ISO 28000:2022's effectiveness in enhancing supply chain resilience involves evaluating how well it contributes to the ability of organizations to withstand disruptions and recover swiftly. Key points to consider include:

Risk Assessment and Mitigation: A core tenet of ISO 28000:2022 is the emphasis on systematic risk assessment (International Organization for Standardization, 2022). By proactively identifying potential threats and vulnerabilities throughout the supply chain, organizations can implement mitigation strategies to minimize disruptions (Sodhi et al., 2018). This proactive approach is essential for building resilience, as it allows organizations to prepare for and respond to unexpected events more effectively.

Business Continuity Planning: The standard places importance on developing and maintaining a business continuity plan (BCP) (International Organization for Standardization, 2022). A robust BCP outlines strategies for recovering from disruptions and ensuring business continuity during crises. Organizations that implement ISO 28000:2022 are more likely to have well-defined BCPs in place, enabling them to adapt and recover more swiftly from disruptions, thereby enhancing supply chain resilience.

Collaboration and Communication: Effective collaboration and communication among supply chain partners are critical for building resilience (Christopher, 2016). ISO 28000:2022 encourages collaboration by promoting information sharing and joint risk management initiatives with suppliers and

The literature review revealed that ISO 28000 implementation has a positive impact on supply chain resilience. The standard's emphasis on risk mitigation, collaboration, and continuous improvement resonates with established principles for building resilient supply chains (Sodhi et al., 2018; Christopher, 2016; Gunasekaran et al., 2019). However, a significant gap exists in empirical studies directly measuring the impact of ISO 28000:2022 on objective metrics of resilience (e.g., recovery time, cost reductions).

4.2 Role of ISO 28000:2022 in Mitigating Security Risks within the Supply Chain

The focus on risk assessment and management within ISO 28000:2022 offers a valuable framework for evaluating security vulnerabilities throughout the supply chain (International Organization for Standardization, 2022).

Security Management System: The standard establishes a systematic approach to security management (International Organization for Standardization, 2022). Organizations that adopt ISO 28000:2022 can implement a comprehensive security management system (SMS) that incorporates policies, procedures, and controls to safeguard against security threats. This systematic approach ensures consistent security practices throughout the organization and strengthens overall supply chain resilience.

Risk-Based Approach: ISO 28000:2022 guides organizations in adopting a risk-based approach to security management (International Organization for Standardization, 2022). This approach involves assessing security risks, identifying critical assets, threat scenarios, and potential vulnerabilities. By prioritizing efforts based on risk level, organizations can allocate resources more effectively and focus on mitigating the most significant threats to their supply chain.

Supply Chain Visibility: The standard promotes transparency by encouraging supply chain partners to share security-related information (International Organization for Standardization, 2022). Enhanced visibility across the supply chain allows for the identification of potential vulnerabilities throughout the network. By fostering information sharing, organizations can collaborate more effectively to address security gaps and strengthen security measures across the entire supply chain, ultimately contributing to greater resilience.

4.3 Challenges and Success Factors Associated with ISO 28000:2022 Implementation

The limited body of research on implementing ISO 28000:2022 makes it difficult to definitively identify key challenges and success factors. However, some potential considerations based on existing knowledge include:

4.3.1 Challenges

- a. **Resource Constraints:** Implementing ISO 28000:2022 requires resources (financial, human, and technological). Organizations may face challenges in allocating sufficient resources.
- b. **Resistance to Change:** Stakeholders may resist changes in processes or practices. Overcoming this resistance is essential for successful implementation.

- c. Complexity: ISO 28000:2022 involves multiple components (risk assessment, security controls, audits). Managing complexity can be challenging.
- d. The challenge of achieving effective collaboration with all supply chain partners.

4.3.2 Success Factors

- a. Leadership Commitment: Strong leadership support is critical. Leaders who champion ISO 28000:2022 create a culture of security awareness.
- b. Training and Awareness: Educating employees and partners about the standard ensures effective implementation.
- c. Integration with Existing Systems: Organizations that integrate ISO 28000:2022 with existing management systems (e.g., ISO 9001 or ISO 14001) tend to succeed.
- d. A comprehensive understanding of the organization's specific security risks.
- e. Engagement and collaboration with all stakeholders across the supply chain.

5 Discussion

5.1 Interpretation of Results

The findings from this qualitative analysis shows that ISO 28000:2022 has the potential to be a valuable tool for organizations seeking to strengthen their supply chain security and resilience. The standard's focus on risk management, collaboration, and continuous improvement aligns with established best practices for building resilient supply chains. However, the limitations in current research necessitate further investigation to definitively assess the standard's effectiveness in enhancing objective metrics of resilience.

5.2 Implications

This study contributes to the academic literature by providing insights into the relationship between ISO 28000 and supply chain resilience. It advances the understanding of the mechanisms through which ISO 28000 influences supply chain security and resilience, offering valuable theoretical insights for future research in this area.

5.3 Limitations

Despite its contributions, this study has several limitations that should be acknowledged: The study's scope is limited to a qualitative analysis of existing literature, which may restrict the depth of analysis.

6. Conclusion

This study explored existing scholarly literature and industry publications to investigate the potential impact of ISO 28000:2022 on supply chain resilience. The findings revealed that the standards emphasis on risk management, collaboration, and continuous improvement aligns with established principles for building resilient supply chains (Sodhi et al., 2018; Christopher, 2016; Gunasekaran et al., 2019).

References

- Ballou, R. H. (2007). The evolution and future of logistics and supply chain management. *European business review*, 19(4), 332-348.
- Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99-120.

- Bellantoni, N., Toker, R., & Van Wassenhove, L. N. (2020). The trade-off between responsiveness and efficiency in a global supply chain: A simulation study. *Production and Operations Management*, 29(6), 1422-1441.
- Christopher, M. (2016). *Logistics & supply chain management* (5th ed.). Pearson Education.
- Closs, D. J., &McGarrell, E. F. (2004). *Strategic supply chain management: A handbook for senior executives*. Kogan Page Publishers.
- DNV. (2023, January 19). ISO 28000 – Supply chain security management. <https://www.dnv.com/services/iso-28000-supply-chain-security-management-4344/>
- Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, 17(Winter Special Issue), 109-122.
- Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, 17(Winter Special Issue), 109-122.
- Gunasekaran, A., Lai, P. C., & Cheng, T. (2019). Building resilience in global supply chains through information technology. *International Journal of Production Economics*, 210, 10 – 23. <https://doi.org/10.1016/j.ijpe.2018.08.008>
- International Organization for Standardization. (2022). ISO 28000:2022 Security and resilience – Security management systems – Requirements (Second edition). <https://www.iso.org/standard/73009.html>
- Jüttner, U., Christopher, M., & Jahre, M. (2003). Supply chain management: A strategic perspective. Thomson Learning
- Ketchen Jr., D. J., &Giunipero, L. C. (2004). The moderating effect of international experience on strategic alliance formation and performance. *Journal of Management*, 30(6), 853-877.
- Ketchen Jr., D. J., &Hult, G. T. M. (2006). In quest of theoretical innovation: A critical analysis of knowledge creation research in international business. *Academy of Management Review*, 31(4), 790-804.
- Langley, R. J., & Parker, E. A. (1982). Equivalent circuit model for arrays of square loops. *Electronics Letters*, 18, 294-296.
- Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*, 22(2), 1-25.
- Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*, 22(2), 1-25.
- Monczka, R. M., Petersen, K. J., Handfield, R. B., & Ragatz, G. L. (1998). Success factors in strategic supplier alliances: the buying company perspective. *Decision sciences*, 29(3), 553-577.
- PECB. (2023, January 11). ISO 28000 Supply Chain Security Management System - EN. https://pecb.com/pdf/brochures/4/iso-28000-lead-implementer_4p.pdf
- Polit, D. F., & Beck, C. T. (2014). *Nursing research: Principles and methods (9th ed.). Wolters Kluwer Health.
- Sodhi, M. S., & Tang, C. S. (2018). Corporate social sustainability in supply chains: a thematic analysis of the literature. *International Journal of Production Research*, 56(1-2), 882-901.

Thijs Willaert. (2022). Revision of the supply chain security standard: What changes in ISO 28000:2022? <https://www.dqsglobal.com/en-us/learn/blog/revision-of-the-supply-chain-security-standard-what-changes-in-iso-28000-2022>