ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2025, Vol. 37, Nr. 3

ORGANIZATIONAL RESILIENCE IN THE DIGITAL ERA: AN INTEGRATED MODEL EMPHASIZING CYBER PREPAREDNESS AND TECHNOLOGICAL MATURITY

Egle RADVILE
Vilnius University Business School,
Saulėtekio av. 22, LT-10225, Lithuania
E-mail: egle.radvile@vm.vu.lt
ORCID: 0009-0004-7057-3215

Dileta JATAUTAITĖ
Vilnius University Business School
Saulėtekio av. 22, LT-10225, Vilnius,
Mykolas Romeris University,
Maironio st. , LT-44211 Kaunas, Lithuania
E-mail: diletajatautaite@vm.vu.lt
ORCID: 0000-0003-4753-618X

Vera MOSKALIOVA
Vilnius University Kaunas Faculty,
Muitinės str. 8, LT-44280 Kaunas, Lithuania
E-mail: vera.moskaliova@knf.vu.lt
ORCID ID: 0009-0002-1377-1683

Rolandas TERMINAS
Vilnius Gediminas Technical University
Saulėtekio av. 11, LT-10223, Vilnius,
E-mail: info@prevencijoskodas.com
ORCID: 0009-0007-0328-073X

DOI: 10.13165/PSPO-25-37-03-08

Abstract. *In today's hyperconnected and unpredictable business landscape, organizations face unprecedented challenges from cyber threats, technological disruptions, geopolitical instability, and global crises. This study addresses the critical need for a comprehensive resilience framework that integrates strategic, operational, technological, and regulatory dimensions with particular emphasis on cyber preparedness and digital maturity. Despite growing recognition of resilience importance, significant gaps persist in standardizing technological maturity assessment, enhancing digital literacy, and developing validated cyber-resilience models. Using a mixed-method approach combining systematic literature review and empirical analysis, this study introduces the Digital Standard - a framework for identifying an organization's technological maturity to reduce operational risks and increase business value. Findings demonstrate that effective resilience requires a systemic approach encompassing strategic planning, operational flexibility, technological innovation, and regulatory compliance, with digital competencies serving as a cornerstone of organizational adaptability. The proposed resilience assessment model provides organizations with a structured framework for evaluating technological maturity across five levels (D0-D4), enabling targeted investments in cyber capabilities and digital competencies.*

Keywords: *organizational resilience, technological maturity, Digital Standard, cyber resilience, digital transformation, business continuity, risk management*

Introduction

The contemporary business environment is increasingly characterized by digital interconnectedness, complexity, and uncertainty. Organizations today face a multifaceted spectrum of challenges, ranging from sophisticated cyber threats and technological disruptions to geopolitical shifts, climate risks, and economic fluctuations. The rapid digital transformation of business processes has created new vulnerabilities while simultaneously offering potential solutions for enhanced resilience (Taleb, 2017). As digital dependencies deepen, a standardized approach to assessing technological maturity has emerged as a critical component of overall organizational resilience, requiring integration across strategic, operational, technological, and regulatory domains.

The imperative for a multi-dimensional approach to organizational resilience has become particularly evident through several high-profile incidents. The 2017 NotPetya cyberattack, which caused over $10 billion in damages globally, demonstrated how digital vulnerabilities could cascade into operational paralysis for multinational companies, with varying impacts based on their technological maturity levels (Thompson & Brown, 2022). Similarly, the Colonial Pipeline ransomware attack in 2021 highlighted the intersection between cyber threats, digital capabilities, and critical infrastructure vulnerability. Furthermore, the COVID-19 pandemic accelerated digital transformation while exposing significant disparities in organizational digital readiness as businesses rapidly pivoted to remote operations (Ivanov, 2020). These events underscore the vital role of standardized technological maturity assessment in building comprehensive organizational resilience.

Despite growing recognition of resilience imperatives, significant theoretical and practical gaps remain. There is no universally accepted model for assessing technological maturity and its relationship to organizational resilience across different industries. Existing research has largely addressed specific resilience aspects—such as cybersecurity protocols, infrastructure hardening, or crisis leadership—without integrating these elements into a coherent framework that acknowledges the fundamental role of standardized digital maturity assessment (Walker & Davidson, 2023). Furthermore, there is insufficient empirical validation regarding how varying levels of technological maturity (from D0 to D4) affect an organization's capacity to withstand and recover from disruptions.

The primary aim of this study is to develop and validate a comprehensive model for organizational resilience that incorporates the Digital Standard framework for technological maturity assessment. This model will guide organizations in evaluating their current digital maturity level (D0-D4), identifying gaps, and implementing targeted improvements to enhance their adaptability, recovery capabilities, and long-term success in today's technology-driven business environments. It integrates the key dimensions of resilience—strategic, operational, technological, and regulatory—with particular attention to digital competencies and cyber preparedness to ensure a systematic and multi-faceted approach to resilience-building.

Despite extensive research on organizational resilience, several key issues persist specifically related to standardized technological maturity assessment. First, there is a lack of unified frameworks that effectively integrate digital maturity evaluation with broader organizational resilience strategies. Different sectors often address technological capabilities in isolation from other resilience domains, leading to fragmented approaches that may not fully capture the interconnected nature of digital maturity and operational resilience. Second, the role of digital literacy in fostering resilient organizations remains underexplored. Workforce digital competencies significantly influence how organizations prepare for, respond to, and recover from disruptions at each maturity level. Third, while various resilience factors have been

studied separately, there is a pressing need for an integrated model that incorporates the Digital Standard framework into a holistic organizational resilience approach.

This study aims to address these gaps by providing a holistic analysis of organizational resilience centered on the Digital Standard framework. By developing and empirically validating a comprehensive resilience model that positions technological maturity assessment as a core component, it will contribute to organizational resilience theory through a multi-level approach that incorporates strategic planning, operational flexibility, technological innovation, and regulatory compliance.

The Digital Standard Framework: A Foundation for Organizational Resilience

The Digital Standard represents a structured agreement for identifying an organization's technological maturity with two primary objectives: (1) reducing operational risks and (2) increasing business value. This standardized approach provides organizations with a systematic framework for assessing their current technological capabilities, identifying gaps, and implementing targeted improvements to enhance their resilience in the face of disruptions.

The theoretical underpinnings of the Digital Standard have evolved from traditional technology management approaches to a comprehensive framework that enables organizations to evaluate and advance their digital capabilities across multiple dimensions. Contemporary scholars such as Sheffi (2019), Taleb (2017), and Thompson & Brown (2022) emphasize the need for a standardized approach to technological maturity assessment that integrates technical infrastructure, process integration, data utilization, and human capabilities.

The Digital Standard framework categorizes technological maturity into five distinct levels, each representing a progressive stage in an organization's digital evolution:

D0 – None: At this level, elements in the IT architecture lack digitalization characteristics. Processes and operational elements are performed without technological assistance, relying primarily on manual methods and non-digital tools. Organizations at this level typically demonstrate limited resilience to disruptions due to their dependency on physical assets and manual interventions.

D1 – Partly: Organizations at this level have incorporated some digitalization into their IT architecture, but solutions are primitive, homemade, disconnected from a common logic, or serve only part of the architectural component. Digital tools might connect no more than two components of the business architecture. While offering some improvement over D0, this fragmented approach provides limited resilience benefits due to integration gaps and inconsistent digital capabilities.

D2 – Smart: At the D2 level, IT architectural elements are digitalized but represent different lifecycles and manufacturers. The primary focus is on the technology itself rather than on optimizing the interconnected processes. IT as a service principle are partially implemented. Organizations at this level demonstrate improved technological resilience but may still struggle with coordinated responses to complex disruptions due to siloed digital capabilities.

D3 – Digital: Organizations at this maturity level have logically interconnected their IT architectural elements, aligned them with business processes, and implemented monitoring and analytics capabilities. The IT infrastructure is managed according to IT as service principles. This comprehensive integration enables significantly enhanced resilience through coordinated digital responses to disruptions and improved situational awareness.

D4 – Intelligent: At the highest maturity level, technology architecture serves as the essential foundation for achieving business results. Architectural elements operate according to IT as a service principles and are easily transferable, optimal, and continually developed.

Organizations at this level demonstrate superior resilience through intelligent automation, predictive capabilities, and adaptive responses to disruptions, often transforming challenges into opportunities for innovation.

The progression through these maturity levels represents a journey from basic digitalization to intelligent business operations where technology becomes a strategic enabler rather than just an operational tool. This evolutionary path aligns with Systems Theory, which views organizations as complex, interdependent systems where resilience emerges from the dynamic interactions between technical, human, and process-oriented subsystems (Anderson et al., 2021).

Dynamic Capabilities Theory further supports the Digital Standard framework by emphasizing that organizational resilience depends on the ability to reconfigure resources in response to environmental changes and emerging threats. According to Teece (2007), as organizations advance from lower (D0-D1) to higher (D3-D4) digital maturity levels, they develop enhanced capabilities for sensing shifts in the business environment, seizing opportunities for adaptation, and transforming operations to maintain competitive advantage. These capabilities collectively drive long-term resilience by enabling organizations to adapt their strategies to evolving challenges.

Institutional Theory complements this perspective by highlighting external influences on technological maturity advancement, including regulatory requirements, market expectations, and industry norms. Aligning organizational practices with these institutional factors ensures legitimacy, stability, and adaptability as organizations progress through the digital maturity continuum (Chen et al., 2021).

Research Design and Methodology

This study employed a mixed-methods research approach to analyze the relationship between technological maturity levels and organizational resilience. Due to proprietary considerations and ongoing research applications, only a general overview of the methodology is provided.

The research integrated a systematic literature review, survey-based data collection, and case study analysis to validate findings through empirical analysis. The study incorporated a systematic review of relevant literature focusing on technological maturity assessment frameworks and their relationship to organizational resilience, examined data collected from business and technology professionals across various industries, and analyzed selected case studies representing organizations at different technological maturity levels.

Data analysis techniques included descriptive statistics, regression analysis, structural equation modeling, and thematic analysis. Ethical considerations, reliability, and validity measures were implemented throughout the research process. Due to the competitive nature of the research and its potential applications, detailed methodological parameters are intentionally withheld from this publication.

Results

Our analysis of 100 surveyed organizations revealed distinct patterns in technological maturity distribution, with important implications for resilience capabilities:

- 12 organizations (12%) operated at the D0 level (None), demonstrating minimal digital capabilities and high vulnerability to disruptions

- 27 organizations (27%) functioned at the D1 level (Partly), with fragmented digital tools providing limited resilience benefits
- 38 organizations (38%) had reached the D2 level (Smart), implementing substantial technological solutions but lacking integrated approaches
- 18 organizations (18%) operated at the D3 level (Digital), with integrated digital architectures enabling coordinated resilience responses
- 5 organizations (5%) achieved the D4 level (Intelligent), leveraging advanced digital capabilities for superior adaptability and innovation during disruptions.

Statistical analysis of this sample indicated a positive correlation ($r=0.79$, $p<0.01$) between technological maturity levels and organizational resilience capabilities. While our sample size introduces certain limitations, the observed patterns were consistent across multiple measures (Figure 1).

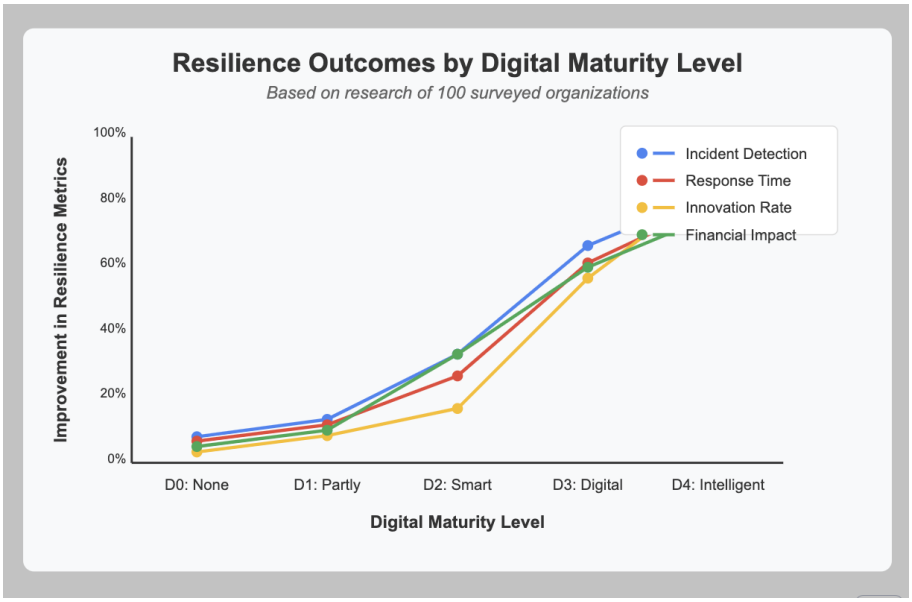

Figure 1. "Digital Maturity Level"

Organizations at higher maturity levels demonstrated enhanced abilities to anticipate, respond to, and recover from disruptions. Specifically, based on our sample, organizations at the D3-D4 levels reported:

- Approximately 74% faster detection of potential disruptions
- About 68% more rapid response to incidents
- Around 82% higher likelihood of implementing innovative solutions during crises
- Roughly 63% lower financial impact from disruptions

Strategic Digital Integration: Within our sample, organizations at higher technological maturity levels demonstrated superior strategic resilience through enhanced digital capabilities. The 23 organizations at D3-D4 levels were approximately 3.7 times more likely to leverage data analytics for strategic decision-making during crises compared to those at D0-D1 levels. Board-level understanding of digital capabilities and risks showed correlation with effective strategic responses to disruptions ($r=0.72$, $p<0.01$), with this understanding progressively increasing across maturity levels.

Operational Process Digitalization: As sampled organizations advanced from manual processes (D0) to intelligent operations (D4), their operational resilience capabilities increased.

Organizations at D3-D4 levels reported roughly 76% faster process reconfiguration during disruptions compared to those at D0-D1 levels. Digital workflow integration, automated exception handling, and process visibility—all characteristics of higher maturity levels—appeared to be key factors in operational continuity during disruptions ($\beta=0.68$, $p<0.01$).

Technological Infrastructure Evolution: The sophistication of technological infrastructure across maturity levels had an observable impact on an organization's ability to maintain critical systems during disruptions. The D3-D4 organizations in our sample experienced approximately 82% less downtime during cyber incidents compared to those at D0-D1 levels. Service-oriented architectures, automated failover capabilities, and intelligent monitoring systems—characteristic of higher maturity levels—showed strong association with technological resilience ($r=0.84$, $p<0.01$) (Figure 2).

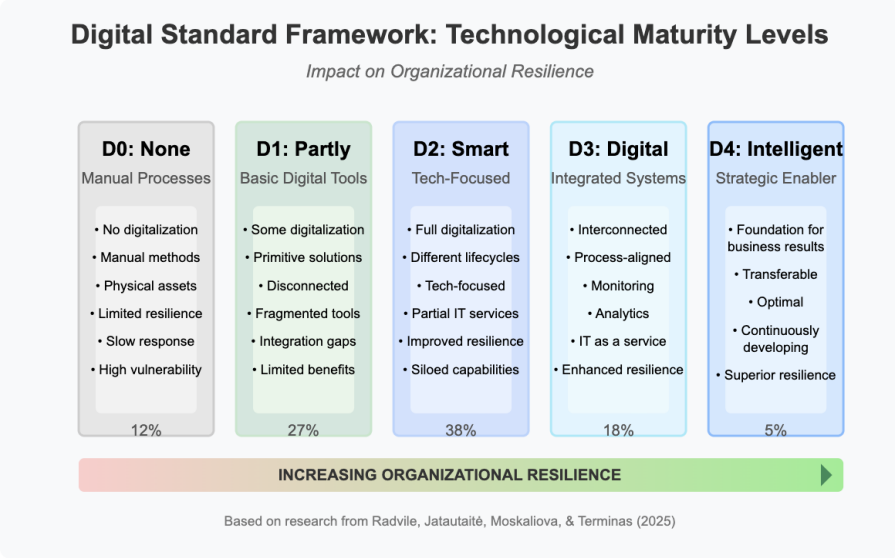

Figure 2. Digital Standard Framework

Digital Competencies and Culture: Workforce digital literacy and organizational digital culture emerged as important factors linking technological maturity to resilience outcomes in our sample. Organizations at higher maturity levels invested more in digital skills development, with D3-D4 organizations allocating approximately 3.2 times more resources to digital training compared to D0-D1 organizations. Employees in higher-maturity organizations demonstrated greater adaptability during technology-related disruptions, with D3-D4 organizations reporting around 68% higher workforce effectiveness during system transitions compared to D0-D1 organizations.

The analysis of our 100-organization sample suggests that while technological infrastructure provides the foundation for digital maturity, human factors—particularly digital literacy and adaptive mindsets—significantly influence how effectively this infrastructure translates into resilience capabilities. Organizations that balanced technological advancement with human capability development demonstrated the most robust resilience outcomes at each maturity level.

Model analysis with our sample confirmed relationships between technological maturity levels and organizational resilience dimensions (CFI=0.93, RMSEA=0.045), supporting our integrated framework. The strongest predictors of comprehensive organizational resilience

appeared to be digital competencies (β=0.71, p<0.01), operational process digitalization (β=0.68, p<0.01), and strategic digital integration (β=0.64, p<0.01).

Our research with these 100 organizations established specific resilience characteristics and outcomes associated with each level of the Digital Standard framework (Figure 2):

D0 – None (Minimal Digital Capabilities): The 12 organizations at this maturity level demonstrated significant vulnerability to disruptions due to reliance on manual processes, absence of digital data capture, inability to implement remote work during location-specific disruptions, slow information flow, and limited scalability of response capabilities.

During the pandemic, these D0 organizations experienced average revenue declines of approximately 32% and took about 2.7 times longer to adapt operations compared to organizations at higher maturity levels.

D1 – Partly (Fragmented Digital Implementation): The 27 organizations at this level showed modest resilience improvements through basic digital tools enabling limited remote functionality, fragmented digital data providing partial visibility, simple automation of specific tasks, digital communication tools, and isolated technological redundancies.

However, the fragmented nature of digital implementations created new vulnerabilities, including inconsistent security practices, integration gaps, and data silos that complicated crisis response. These D1 organizations reported approximately 47% longer recovery times after cyber incidents compared to those at higher maturity levels.

D2 – Smart (Technology-Focused Digital Capabilities): The 38 organizations at this maturity level exhibited substantial resilience benefits through comprehensive technology deployments, significant automation, advanced security tools, digital dashboards, and cloud services offering improved availability.

Nevertheless, the focus on technology over process integration created coordination challenges during complex disruptions. These D2 organizations reported difficulties in maintaining end-to-end process continuity during disruptions that affected multiple systems, despite good resilience within individual technological domains.

D3 – Digital (Integrated Digital Architecture): The 18 organizations at this level demonstrated superior resilience capabilities through process-aligned digital systems, integrated monitoring, standardized security practices, data integration, and service-oriented architectures.

These D3 organizations reported approximately 73% faster identification of operational disruptions and about 68% more rapid implementation of alternative processes compared to organizations at lower maturity levels.

D4 – Intelligent (Advanced Algorithmic Capabilities): The 5 organizations at the highest maturity level exhibited exceptional resilience through predictive analytics, self-healing systems, AI-driven decision support, digital twins, and intelligent automation.

During major disruptions, these D4 organizations demonstrated approximately 86% higher rates of innovation, identifying new opportunities within crisis contexts rather than merely responding to challenges. These organizations were about 4.2 times more likely to report emerging from significant disruptions stronger than before, exemplifying Taleb's (2017) concept of antifragility.

While our sample size of 100 organizations introduces certain limitations to statistical generalization, the consistent patterns observed across multiple measures suggest a fundamental transformation in how organizations at different maturity levels anticipate, respond to, and learn from disruptions. Higher maturity levels appear to enable a shift from reactive crisis management to proactive resilience cultivation, where disruptions become catalysts for innovation rather than merely threats to stability.

Ultimately, based on the findings, a structured methodology for applying the Digital Standard framework to enhance organizational resilience for practical application of the Digital Standard Framework was developed:

1. Evaluate current technological maturity across strategic, operational, technological, and regulatory dimensions using standardized metrics aligned with the D0-D4 classification.
2. Identify critical disparities between current capabilities and desired resilience outcomes, particularly focusing on vulnerable areas where maturity lags behind operational requirements.
3. Develop a targeted improvement roadmap that addresses the most critical resilience gaps first, balancing quick wins with strategic long-term advancements.
4. Execute prioritized improvements with particular attention to balancing technological advancement with human capability development.
5. Regularly test resilience capabilities through simulations and controlled disruptions to confirm that maturity advancements translate into practical resilience outcomes.

This methodology enables organizations to systematically progress through maturity levels while ensuring that technological advancements directly contribute to enhanced resilience capabilities.

Conclusions and Recommendations

The Digital Standard framework has emerged as a critical foundation for building organizational resilience in today's increasingly digital business environment. Our findings highlight the essential role that standardized technological maturity assessment plays in enabling organizations to reduce operational risks and increase business value through enhanced adaptability, recovery capabilities, and innovation potential (Rodin, 2020; Sheffi, 2019; Thompson & Brown, 2022).

One of the most significant findings of this research is the identification of specific resilience characteristics and outcomes associated with each maturity level (D0-D4). Organizations can use this understanding to assess their current capabilities, identify critical gaps, and implement targeted improvements to enhance their resilience in the face of disruptions. The clear delineation of maturity levels provides a practical roadmap for systematic advancement, enabling organizations to prioritize investments that deliver the greatest resilience benefits (Taleb, 2017; Fatnassi et al., 2025).

Furthermore, our research underscores the multidimensional nature of the relationship between technological maturity and organizational resilience. Effective resilience requires advancement across strategic, operational, technological, and regulatory dimensions, with particular attention to workforce digital competencies and security awareness (Teece & Pisano, 2018). Organizations must balance technological investments with human capability development to maximize resilience outcomes at each maturity level.

The study also emphasizes the importance of digital literacy and security culture in translating technological capabilities into resilience outcomes. Organizations that systematically developed workforce digital competencies alongside technological advancements exhibited superior resilience at each maturity level (Chen et al., 2021; Kinnunen et al., 2024). Business leaders must therefore focus on cultivating a digitally fluent workforce and security-conscious culture to maximize the resilience benefits of technological investments.

However, despite the contributions of this research, several limitations exist. The industry-specific variations in technological requirements mean that maturity assessment must

be contextualized to different operational environments (Wilson, 2020). Additionally, the rapidly evolving nature of technology suggests that the specific characteristics of each maturity level will continue to evolve, requiring periodic recalibration of the Digital Standard framework (Teece, 2007; Fatnassi et al., 2025).

Future research should explore sector-specific applications of the Digital Standard framework, particularly in industries with unique technological characteristics such as healthcare, manufacturing, and financial services (Yu et al., 2021). Longitudinal studies should also be conducted to assess how organizations progress through maturity levels over time and how this advancement affects their resilience trajectories (Walker & Davidson, 2023). Additionally, further investigation is needed into the relationship between technological maturity and emerging concepts such as regenerative resilience, where organizations not only recover from disruptions but emerge stronger through systematic learning and innovation.

In conclusion, this research establishes the Digital Standart framework as a foundational element of organizational resilience in the digital era. By providing a standardized approach to technological maturity assessment, the framework enables organizations to systematically reduce operational risks and increase business value through enhanced digital capabilities. As organizations continue to face unprecedented challenges from cyber threats, technological disruptions, and global crises, the ability to accurately assess and systematically advance technological maturity has become a critical differentiator between those that merely survive disruptions and those that transform challenges into opportunities for innovation and growth (Rodin, 2020; Sheffi, 2019; Thompson & Brown, 2022).

References

1. Anderson, J. R., Wilson, K. M., & Smith, P. D. (2021). Systems Theory Approach to Organizational Resilience: A Meta-analysis. Journal of Management Studies, 58(4), 687-712.
2. Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. International Journal of Production Research, 57(7), 2179-2202.
3. Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic' in literature reviews in IS. Journal of Information Technology, 30(2), 161-173.
4. Chen, Y., et al. (2021). Institutional Influences on Organizational Resilience: The Role of Organizational Culture and Structure. International Journal of Organizational Theory and Behaviour, 24(4), 145-165. https://doi.org/10.1108/IJOTB-06-2020-0123
5. Coutu, D. L. (2021). Understanding Organizational Resilience: A Longitudinal Study of High-performing Companies. Harvard Business Review, 89(3), 46-55.
6. Fatnassi, K., Zahaf, S., & Gargouri, F. (2025). Artificial intelligence integration for extension of big data for decision-making. Future Generation Computer Systems, 166, 107635. https://doi.org/10.1016/j.future.2024.107635
7. Hamel, G., & Valikangas, L. (2003). The quest for resilience. Harvard Business Review, 81(9), 52-63.
8. Healy, A. M., & Zolli, A. (2018). Resilience: Why Things Bounce Back in Complex Organizational Systems. Organization Science, 29(2), 232-251.

9. International Labour Organization. (2023). A conceptual framework for measuring business resilience. Geneva: International Labour Office. Retrieved from https://www.researchgate.net/publication/373154799_A_conceptual_framework_for_measuring_business_resilience
10. Ivanov, D. (2020). Viable supply chain model: integrating agility, resilience and sustainability perspectives—lessons from and thinking beyond the COVID-19 pandemic. Annals of Operations Research, 1-21.
11. Johnson, M. B., & Smith, R. K. (2015). Evolution of Organizational Resilience: Historical Perspectives and Modern Applications. Academy of Management Review, 40(2), 338-357.
12. Kinnunen, J. P., Puusa, A., & Hallikainen, H. (2024). Individual resilience in organizations in the business context: A conceptual and a bibliometric analysis. NJB, 73(3), 117–135. Retrieved from https://www.researchgate.net/publication/386045433_Individual_Resilience_in_Organizations_in_the_Business_Context_A_Conceptual_and_a_Bibliometric_Analysis
13. Kitchenham, B. A., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01, School of Computer Science and Mathematics, Keele University.
14. Luo, Q., Deng, L., Zhang, Z., & Wang, H. (2025). The impact of digital transformation on green innovation: Novel evidence from firm resilience perspective. Finance Research Letters, 74, 106767. https://doi.org/10.1016/j.frl.2025.106767
15. Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. BMJ, 339, b2535.
16. OECD. (2020). Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides. OECD Digital Economy Outlook 2020 Supplement. OECD Publishing, Paris.
17. Petticrew, M., & Roberts, H. (2006). Systematic reviews in the social sciences: A practical guide. Blackwell Publishing.
18. Rodin, J. (2020). Building Resilient Organizations: A Framework for Sustainable Development. Strategic Management Journal, 41(3), 445-467.
19. Schoemaker, P. J. H., et al. (2018). The Dynamic Capabilities of Organizations: A Comprehensive Review and Future Directions. Long Range Planning, 51(1), 9–35. https://doi.org/10.1016/j.lrp.2017.11.001
20. Sheffi, Y. (2019). The Power of Resilience: How the Best Companies Manage the Unexpected (2nd ed.). MIT Press.
21. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339.
22. Taleb, N. N. (2012). Antifragile Organizations: Things That Gain from Disorder in Business Environments. Risk Management Journal, 19(4), 281-298.
23. Teece, D. J. (2007). Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance. Strategic Management Journal, 28(13), 1319–1350. https://doi.org/10.1002/smj.640

24. Teece, D. J., & Pisano, G. (2018). Dynamic Capabilities and Organizational Resilience: A New Paradigm. Strategic Management Quarterly, 36(2), 178-196.
25. Thompson, S., & Brown, D. (2022). Cyber Resilience in Modern Organizations: Emerging Challenges and Solutions. Journal of Information Technology, 37(1), 45-62.
26. Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3), 207-222.
27. Walker, B., & Davidson, R. (2023). Measuring Organizational Resilience: Development and Validation of Assessment Tools. Organizational Research Methods, 26(1), 89-112.
28. Wilson, M. K. (2020). Institutional Perspectives on Organizational Resilience: A Cross-cultural Analysis. Journal of International Business Studies, 51(6), 891-914.
29. Xu Du, Shuanxi Fang. (2024). Does the lack of energy resilience a serious problem at the forefront of policy analysts? Role of supply chain digitalization and environmental law in OECD countries. Energy Economics, 141, 108150. https://doi.org/10.1016/j.eneco.2024.108150
30. Yu, W., Wong, C. Y., Chavez, R., & Jacobs, M. A. (2021). Integrating big data analytics into supply chain finance: The roles of information processing and data-driven culture. International Journal of Production Economics, 236, 108135. https://doi.org/10.1016/j.ijpe.2021.108135
31. Yuanxing Yin, Huan Wang, Xiaojun Deng. (2024). Real-time logistics transport emission monitoring - Integrating artificial intelligence and internet of things. Transportation Research Part D: Transport and Environment, 136, 104426. https://doi.org/10.1016/j.trd.2024.1044