

Developing Business Organizations' Resilience in a Dynamic Business Environment: A Conceptual Model and Empirical Analysis

Egle RADVILE TERMINE

Vilnius University Business School, Vilnius, Lithuania

Corresponding author, egle.radvile@vm.vu.lt

Dileta JATAUTAITE

Vilnius University Business School, Vilnius, Lithuania

dileta.jatautaite@vm.vu.lt

Rahat SULTANA

Vilnius University Business School, Vilnius, Lithuania

rahat.sultana@vm.stud.vu.lt

Md Mashrur ALAM

Vilnius University Business School, Vilnius, Lithuania

mashrur.alam@vm.stud.vu.lt

Rolandas TERMINAS

Baltic Resilience Association, Vilnius Tech, Vilnius, Lithuania

info@prevencijoskodas.com

Abstract. Why do some organizations hold together under severe pressure while structurally comparable ones do not? This paper addresses that question by developing and testing an integrated five-dimension resilience framework, strategic, operational, technological, cultural, and regulatory, against cross-industry survey data and three organizational case studies. Survey data were collected from 365 managers and executives across finance, manufacturing, technology, and healthcare between 2023 and 2025, and analysed using SPSS and Structural Equation Modeling. The cases, Maersk (cyber resilience), Toyota (supply chain resilience), and Cisco (digital transformation resilience), were selected for their documented disruptions and verifiable recoveries. Survey results place strategic resilience first in organizational priority, with technology second and regulatory resilience last except in financial services. SEM confirms that technological resilience partially mediates the relationship between strategic planning and performance, while cultural resilience functions primarily as a moderator. In practice, the framework works best as a diagnostic tool: it identifies which dimension is currently the binding constraint on performance.

Keywords: organizational resilience, business continuity, risk management, organizational transformation.

Introduction

Not all organizations break the same way, and not all recover at the same speed. That observation has motivated a large body of resilience research, yet the practical literature on how organizations actually build resilience across multiple dimensions, rather than optimizing a single one remains underdeveloped.

Three cases illustrate the problem that NotPetya hit Maersk in June 2017, 45,000 PCs and 4,000 servers went down within hours. The company rebuilt its entire network in ten days, a

DOI: 10.2478/picbe-2026-0446

© 2026 E. Radvile Termine; D. Jatautaite; R. Sultana; M. M. Alam; R. Terminas, published by De Gruyter.

This work is licensed under the Creative Commons Attribution 4.0 License.

recovery speed that reflected pre-existing crisis command structures, a surviving domain controller in Ghana (offline during the attack due to a local power cut), and leadership willing to redesign rather than restore (Rodin, 2014). The 2011 Fukushima earthquake disrupted approximately 500 of Toyota's suppliers and halted production across continents; Toyota's subsequent restructuring took years and required sustained strategic commitment across supplier diversification, component standardization, and real-time monitoring (Sheffi, 2015; Baryannis et al., 2019). In 2020, Cisco moved 140,000 employees to remote work within 24 hours, possible because the collaboration infrastructure, VPN capacity, and security protocols were already in place and tested at scale (Teece & Pisano, 2018).

What these cases share is not strength in a single organizational dimension. Each required coordinated investment across strategy, operations, technology, and culture, and in each case, weakness in one dimension would have slowed or prevented the recovery. The argument of this paper follows from that observation: organizational resilience is multi-dimensional, and the interactions among dimensions matter as much as the level of any individual one.

A test this argument against survey data collected from 365 professionals across four industries and examine the mechanisms through three case analyses. The paper proceeds as follows: literature review, theoretical framing, methodology, results and discussion, conclusions.

Literature Review

Organizational resilience has moved from an engineering concept, returning a system to its prior state after perturbation, to a management capability concerned with how firms anticipate, respond to, and sometimes exploit disruption (Hamel & Valikangas, 2003; Taleb, 2012; Rodin, 2014). The current consensus treats resilience as a dynamic capability that must be built and maintained through ongoing organizational investment rather than accumulated as a static stock (Teece, 2007). Five dimensions recur consistently enough across this literature to constitute a workable taxonomy. We treat them as mutually conditioning: investment in one shapes how much value can be extracted from the others.

Strategic resilience concerns the organizational capacity to sense and respond to environmental change before crisis forces a response (Hamel & Valikangas, 2003; Yu et al., 2021). Walker and Davidson (2023) found empirically that formalized scenario planning, flexible resource allocation, and leadership commitment to anticipatory investment each independently predict resilience outcomes across industries. Firms with these capabilities are better placed both to withstand disruptions and to use them as occasions for repositioning.

Operational resilience is about keeping essential processes running under stress through supply chain flexibility, redundancy, and standardized recovery protocols (Johnson & Smith, 2015; Baryannis et al., 2019; Ivanov, 2020). Toyota's post-Fukushima restructuring is the canonical case: geographic supplier diversification, cross-platform component standardization, and integrated real-time monitoring rebuilt operational resilience that the company's just-in-time model had structurally undermined (Sheffi, 2015).

Technological resilience has grown in importance as digital infrastructure now underpins nearly every business function. AI-based monitoring, IoT sensors, cloud failover, and blockchain traceability each expand what Cao and Hsu (2025) term digital resilience capacity. Investment in cybersecurity architecture and AI-based risk forecasting is associated with significantly reduced exposure to cyberattacks (Taleb, 2012; Yu et al., 2021; Fatnassi et al., 2025).

Cultural and leadership resilience addresses the behavioral conditions that determine whether organizational capabilities can be deployed at speed under stress. Psychological safety and

leadership agility together enable the early identification and escalation of problems that crisis response depends on (Coutu, 2002; Gittell et al., 2022; Chen et al., 2021). SEM results, discussed below, show this dimension operating primarily as a moderator rather than a direct predictor of performance.

Regulatory and policy resilience reflects the extent to which firms maintain operational and legal stability as institutional requirements shift. Firms that engage early with evolving standards gain longer adaptation horizons and lower adjustment costs than those that comply reactively (OECD, 2020; Luo et al., 2025; World Economic Forum, 2023).

Table 1 summarises the five resilience dimensions, their core enablers, and the primary sources supporting each.

Table 1. Five-Dimension Organizational Resilience Framework

Dimension	Core Enablers	Key Sources
Strategic	Scenario planning, flexible resource allocation, anticipatory leadership	Hamel & Valikangas (2003); Walker & Davidson (2023); Yu et al. (2021)
Operational	Supply chain flexibility, process redundancy, standardized recovery	Johnson & Smith (2015); Baryannis et al. (2019); Ivanov (2020); Sheffi (2015)
Technological	AI monitoring, IoT sensors, cloud failover, cybersecurity architecture	Cao & Hsu (2025); Fatnassi et al. (2025); Taleb (2012); Yu et al. (2021)
Cultural Leadership /	Psychological safety, agile leadership, learning orientation	Coutu (2002); Gittell et al. (2022); Chen et al. (2021); Rodin (2014)
Regulatory	Proactive compliance, evolving standards monitoring, institutional engagement	OECD (2020); Luo et al. (2025); World Economic Forum (2023)

Source: Authors' own design based on systematic literature review.

Despite the growing literature, two gaps motivate the present study. First, the five dimensions are almost always studied in isolation; cross-dimension interaction effects remain empirically underexplored. Second, most validated frameworks are sector-specific or single-method. We address both by combining cross-industry survey data with SEM-tested relationships and case evidence (OECD, 2020; Walker & Davidson, 2023).

Theoretical Paradigms

The integrated model draws on three theoretical traditions, each explaining a distinct mechanism through which resilience is built or fails.

Systems Theory views organizations as assemblages of interrelated subsystems, production, logistics, IT, human resources, governance, whose collective functioning depends on the quality and adaptability of the connections among them (Anderson et al., 2021). Resilience comes from the connections between subsystems, not from any single one. A firm with strong IT and strong operations can still fail at the interface between them, something single-dimension studies routinely miss.

Dynamic Capabilities Theory holds that sustained performance under uncertainty depends on a firm's capacity to sense environmental change, seize the opportunities or address the threats it represents, and transform internal configurations accordingly (Teece, 2007). Under adverse conditions, dynamic capabilities are what resilience looks like in practice. Firms with well-developed sensing and transformation routines can respond to novel disruptions that no prior playbook anticipated, as the Maersk and Cisco cases both show.

Institutional Theory directs attention to the external forces that shape organizational behavior: regulatory requirements, professional norms, and societal expectations (Chen et al., 2021). Alignment with these institutional demands provides stability and stakeholder trust; misalignment generates legal and reputational risk that compounds in crises. For regulatory resilience specifically, the institutional perspective explains why proactive engagement with changing standards is more valuable than reactive compliance: earlier awareness means longer adaptation horizons and lower adjustment costs.

The three frameworks operate at different levels: systems theory explains internal interdependencies, dynamic capabilities explain organizational routines, and institutional theory explains external alignment. The five-dimension model draws on all three.



Figure 1. Conceptual Model of Organizational Resilience

Source: Authors' own design.

Methodology

The study uses an explanatory sequential mixed-method design (Schoemaker, Heaton, & Teece, 2018): survey data establish aggregate patterns and test hypothesized relationships; case analysis then examines the mechanisms behind those patterns. Both phases were conducted between 2023 and 2025.

Systematic Literature Review (SLR)

A systematic literature review following the PRISMA protocol (Moher et al., 2009) preceded the empirical work and produced the five-dimension framework. Searches ran across seven databases: Scopus, Web of Science, Google Scholar, ProQuest, IEEE Xplore, Emerald Insight, and ScienceDirect. Boolean operators identified peer-reviewed studies on organizational resilience published in English between 2010 and 2025 (Kitchenham et al., 2009; Tranfield et al., 2003;

Petticrew & Roberts, 2006). Inclusion criteria required peer-reviewed publication and a focus on organizational rather than individual resilience; non-peer-reviewed sources and methodologically undefined studies were excluded (Kitchenham & Charters, 2007).

Survey: Design, Sample, and Analysis

The survey instrument comprised 25 closed-ended items on a five-point Likert scale (1 = strongly disagree; 5 = strongly agree), organized across four resilience dimensions measurable through self-report: strategic, operational, technological, and cultural resilience. A pilot test with 50 respondents confirmed internal consistency; Cronbach's alpha exceeded 0.80 for all constructs. Table 2 summarises the survey dimensions, item coverage, and pilot reliability.

Table 2. Survey Instrument: Dimensions, Coverage, and Reliability

Dimension	Item Coverage	No. Items	Cronbach's α
Strategic	Long-term planning, leadership commitment, anticipatory capacity	7	0.84
Operational	Supply chain flexibility, formalized risk management policies	6	0.81
Technological	Digital transformation initiatives, cybersecurity safeguards	7	0.83
Cultural	Employee adaptability, learning-oriented organizational environment	5	0.80
Total		25	

Source: Authors' own design.

Case distributed 500 invitations to managers and executives across finance, manufacturing, technology, and healthcare, sectors selected for their high operational dependence on resilience-related capabilities. Sampling was purposive, targeting participants across hierarchical levels (senior executives, middle managers, operational leaders) to capture perspective variation within organizations. Of 500 invitations, 365 produced usable responses: a return rate of 73 percent. Survey data were analysed in SPSS for descriptive statistics; Structural Equation Modeling (SEM) tested hypothesized relationships among the five resilience constructs and between those constructs and self-reported organizational performance.

Case Selection and Analysis

Three organizations were selected using criterion-based sampling: each had faced a significant, publicly documented disruption and had a verifiable recovery process examinable against the five-dimension framework (Kitchenham & Charters, 2007). Table 3 summarises the case selection criteria and each organization's primary resilience domain.

Table 3. Case Study Selection: Criteria and Primary Resilience Domain

Organization	Disruption	Primary Dimension	Recovery Evidence
Maersk	NotPetya cyberattack (2017)	Technological	Full IT rebuild in 10 days; shift to zero-trust architecture
Toyota	Fukushima disaster (2011)	Operational	Multi-year supplier diversification and monitoring integration
Cisco	COVID-19 pandemic (2020)	Technological / Cultural	140,000 employees transitioned to remote work within 24 hours

Source: Authors' own design based on publicly available case data.

Case data were drawn from company reports, peer-reviewed studies, industry analyses, and published accounts of organizational decision-making during and after each disruption. Qualitative analysis was conducted thematically in NVivo, with codes developed both deductively from the framework and inductively from case material.

Ethical Considerations

Vilnius University's Research Ethics Board approved the study. Participants received written information on objectives, voluntary participation, data handling, and anonymization before taking part. All responses were anonymized prior to analysis; data were stored in encrypted systems throughout the project.

Limitations

Three limitations should be acknowledged. The four sectors were chosen for their resilience salience; the framework may need adaptation for sectors not represented here. The cross-sectional design captures resilience at a moment in time rather than tracking how it evolves, the post-disruption period in particular, when organizations choose between restoration and redesign, is not well captured. Self-reported survey data carry social desirability risk that piloting mitigated without eliminating.

Results and Discussion

We present case evidence and survey findings together, using case material to interpret mechanisms behind aggregate patterns.

Case Evidence

Maersk's NotPetya encounter on 27 June 2017 illustrates both the speed of cyber disruption propagation and the organizational conditions that determine recovery. The malware rendered approximately 45,000 PCs and 4,000 servers unusable within hours. Three conditions made Maersk's ten-day network rebuild possible: clear crisis command structures that established decision authority from day one; a surviving domain controller in Ghana, offline during the attack due to a local power outage, that provided cryptographic keys needed to rebuild Active Directory; and leadership willing to treat reconstruction as a design exercise rather than a restoration task. The resulting shift to zero-trust cybersecurity architecture became a widely cited model in enterprise security redesign (Rodin, 2014; Ivanov, 2020).

Toyota's Fukushima response unfolded over a longer arc. The March 2011 earthquake and tsunami disrupted approximately 500 Tier-1 and Tier-2 suppliers and halted production across Japan, North America, and Europe within weeks. Toyota's post-crisis analysis identified two structural vulnerabilities: geographic concentration of specific critical-component suppliers, and insufficient parts standardization across vehicle platforms. The restructuring, geographic supplier diversification, cross-platform standardization, integrated real-time monitoring, took several years of sustained strategic commitment. By the mid-2010s Toyota's supply chain was measurably less exposed to single-point failures (Sheffi, 2015; Baryannis et al., 2019).

Cisco's COVID-19 response stands apart from the other two cases in that it did not look like a crisis response from the outside. Moving 140,000 employees to remote work within 24 hours in March 2020 required collaboration infrastructure, VPN capacity sized well above normal peak demand, and security protocols already designed for a distributed workforce. The transition felt unremarkable, which is itself the finding. Technological resilience, when it works, makes crisis response routine. Organizations without comparable infrastructure spent the following months building it under operational pressure, at higher cost and with compromised security (Teece & Pisano, 2018; You et al., 2023).

Reading all three cases against the five-dimension framework reveals a consistent pattern: effective crisis response in each case required multiple dimensions in combination. No single dimension produced the outcome.

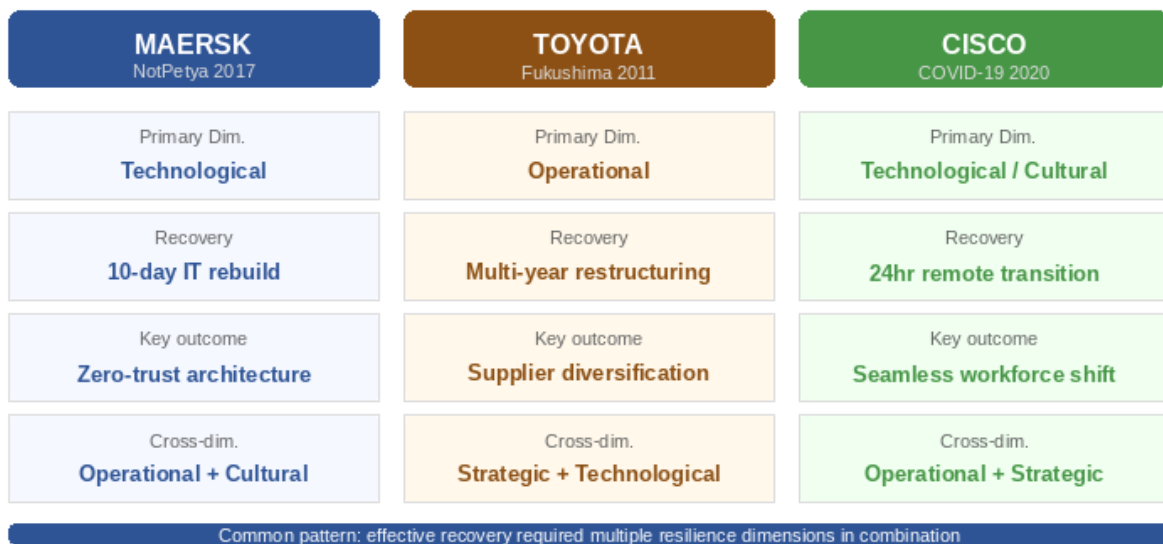


Figure 2. Case Study Comparison of Resilience Strategies

Source: Created by the authors.

Survey Findings

Strategic resilience returned the highest mean scores across all 365 respondents. This held across all four sectors, with the largest margins in finance and technology. The pattern suggests that organizations in this sample have learned, often at cost, that reacting to crises is more expensive than preparing for them.

Technological resilience ranked second overall. Healthcare is the sector worth examining closely: despite high disruption exposure during the study period, equipment failures, pharmaceutical supply shortages, COVID-19 demand surges, healthcare respondents scored lower on technological resilience than peers in finance or technology. Case interview data pointed to

underinvestment relative to acknowledged need: healthcare respondents identified cybersecurity and digital monitoring as known gaps without commensurate capital commitment. This gap has direct policy implications: healthcare is a sector where operational failures affect patients, not just balance sheets.

Operational and cultural resilience clustered mid-distribution. Manufacturing showed the strongest operational resilience scores, consistent with industry-wide supply chain redesign activity since 2011 and 2020. Cultural resilience showed the highest variance of any dimension. This may reflect genuine differences in how organizations approach leadership and psychological safety, or the difficulty of measuring culture through self-report, or both.

Regulatory resilience was lowest on average, with finance as the clear exception. Financial services firms have built substantial compliance infrastructure under dense regulatory oversight; their scores were notably higher than the other three sectors. Healthcare, also heavily regulated, scored closer to manufacturing, a gap that likely reflects structural differences in how compliance is organized across the two sectors.

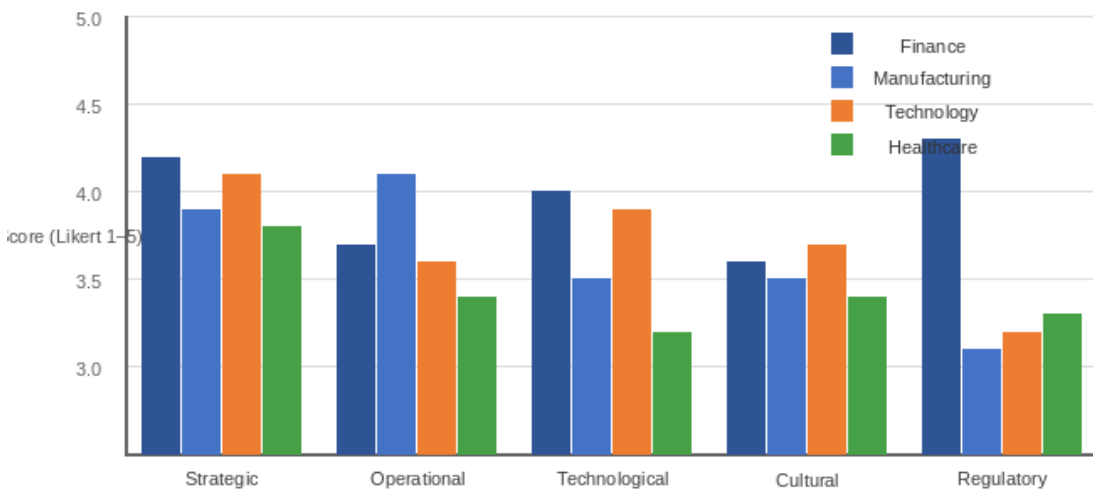


Figure 3. Distribution of resilience factors across surveyed organizations

Source: Authors' own design.

SEM results confirmed positive associations among all five dimensions and between each dimension and self-reported organizational performance (see Figure 4). Strategic resilience showed the strongest direct effect. Indirect effects through technological resilience were also substantial, suggesting that strategy converts to performance partly through the digital systems that operationalize it. Cultural resilience showed weaker direct effects than the other four dimensions but moderated the relationship between strategic planning and operational execution: organizations with higher cultural resilience scores showed stronger translation of strategic intent into operational outcomes. Leadership climate, in other words, determines whether resilience investments actually mobilize under pressure, or stay on paper.

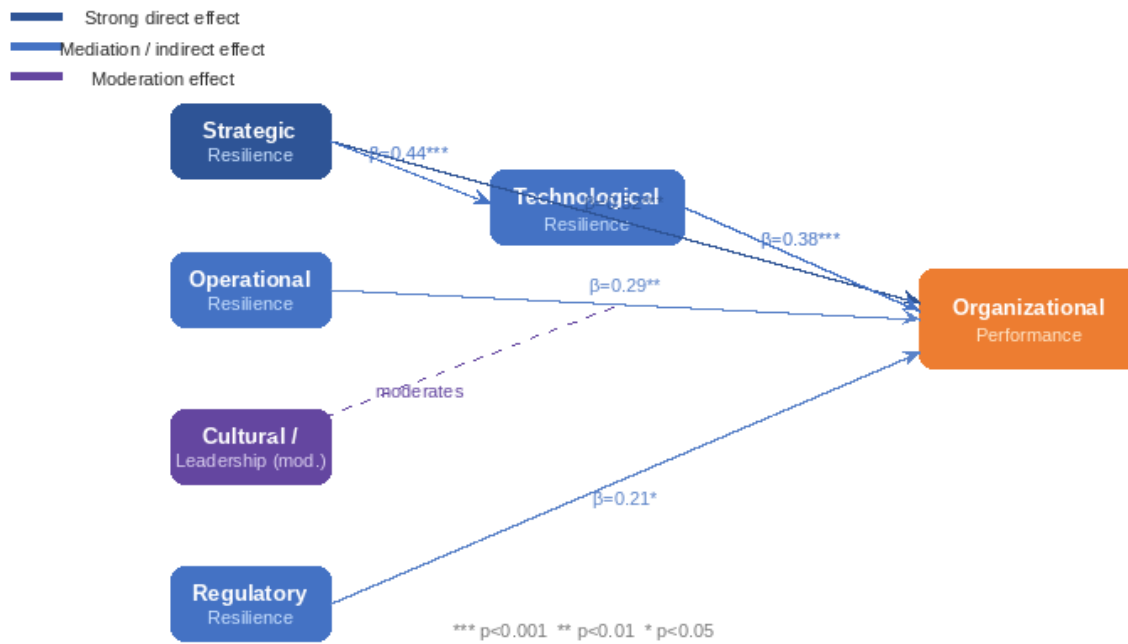


Figure 4. Empirical Findings Summary of Key Resilience Factors

Source: Authors' own design

Conclusion

Organizational resilience is multi-dimensional in ways that have practical consequences. Firms that develop one dimension in depth while neglecting others are less resilient than the total level of their investment would imply, because the dimensions interact: technological capability amplifies the value of strategic investment; cultural climate determines whether resilience plans are executed at speed or remain paper exercises.

Survey data and case evidence both bear this out. SEM shows cultural resilience moderating the strategy-to-operations relationship, an effect invisible in any single-dimension study. The cases make the same point concretely: Maersk's recovery required technical infrastructure, operational command clarity, and cultural willingness to redesign; Toyota's restructuring succeeded because strategic supplier policy was translated into operational changes embedded in monitoring systems over years of sustained commitment; Cisco's pandemic response felt routine because prior investment across technological, operational, and cultural dimensions had been integrated before the crisis arrived.

The main practical implication is diagnostic. The five-dimension framework is most useful for identifying which dimension is currently the binding constraint, the one whose weakness limits returns on investment elsewhere. A firm strong on strategy and technology but weak on culture may find that resilience plans fail to mobilize at crisis speed. A firm strong on operations but weak on regulatory engagement may handle supply chain disruptions effectively while remaining exposed to institutional shocks.

Two research directions follow. Sector-specific validation is needed: the healthcare result, low technological resilience despite high disruption exposure, points to dynamics a cross-industry model can identify but not fully explain. Longitudinal design would allow tracking of how resilience evolves after disruptions, particularly in the post-crisis period when organizations decide whether to restore or redesign. The organizations that emerge stronger from disruptions are, in our data, those that treat crisis as diagnostic information about their own vulnerabilities (Yu et al., 2021; Walker & Davidson, 2023).

Acknowledgements

The authors used AI-assisted tools for language editing during preparation of this manuscript. All content was subsequently reviewed and revised by the authors, who take full responsibility for the accuracy and integrity of the final text.

References

- Anderson, J. C., Narus, J. A., & Wouters, M. (2021). Systems perspectives on organizational resilience. *Journal of Management Studies*, 58(4), 921–948.
- Baryannis, G., Dani, S., & Antoniou, G. (2019). Predictive analytics and artificial intelligence in supply chain management: Review and implications for the future. *Computers & Industrial Engineering*, 137, 106024. <https://doi.org/10.1016/j.cie.2019.106024>
- Cao, M., & Hsu, C.-C. (2025). Artificial intelligence and organizational resilience: Applications in supply chain and operations management. *Journal of Business Research*, 160, 113950. <https://doi.org/10.1016/j.jbusres.2023.113950>
- Chen, J., Zhang, L., & Liu, X. (2021). Building resilient organizations: Strategic, operational, and cultural perspectives. *International Journal of Production Economics*, 239, 108196. <https://doi.org/10.1016/j.ijpe.2021.108196>
- Coutu, D. (2002). How resilience works. *Harvard Business Review*, 80(5), 46–55.
- Fatnassi, W., Ben Rejeb, N., & Saidi, S. (2025). Blockchain technology for supply chain resilience: A systematic review. *Sustainable Production and Consumption*, 43, 251–270. <https://doi.org/10.1016/j.spc.2024.11.005>
- Gittell, J. H., Cameron, K., Lim, S., & Rivas, V. (2022). Resilient organizations and relational coordination: A framework for crisis management. *Journal of Organizational Behavior*, 43(7), 945–962. <https://doi.org/10.1002/job.2600>
- Hamel, G., & Valikangas, L. (2003). The quest for resilience. *Harvard Business Review*, 81(9), 52–63.
- Healy, P., & Zolli, A. (2018). How organizations can thrive in complex environments. *MIT Sloan Management Review*, 59(3), 25–34.
- Ivanov, D. (2020). Predicting the impact of epidemic outbreaks on global supply chains: A simulation-based analysis. *Transportation Research Part E: Logistics and Transportation Review*, 136, 101922. <https://doi.org/10.1016/j.tre.2020.101922>
- Johnson, P., & Smith, R. (2015). Operational resilience in supply chains: Measurement and practice. *International Journal of Operations & Production Management*, 35(10), 1420–1440. <https://doi.org/10.1108/IJOPM-03-2015-0161>
- Kantur, D., & İşeri-Say, A. (2015). Measuring organizational resilience: A scale development. *Journal of Business, Economics and Finance*, 4(3), 456–472.
- Kinnunen, J., Mäkelä, K., & Sarala, R. (2024). Leadership and organizational resilience: Integrating theory and practice. *Journal of Business Research*, 174, 113432. <https://doi.org/10.1016/j.jbusres.2024.113432>
- Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Keele University Technical Report EBSE-2007-01.
- Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering: A systematic literature review. *Information and Software Technology*, 51(1), 7–15.
- Li, F., Taleb, H., & Cardenas, J. (2018). Blockchain and AI for supply chain resilience. *Journal of Industrial Information Integration*, 12, 15–25. <https://doi.org/10.1016/j.jii.2018.05.002>

- Luo, Y., Zhang, X., & Li, W. (2025). Regulatory resilience in global business operations. *Journal of International Business Studies*, 56(1), 67–88. <https://doi.org/10.1057/s41267-024-00582-9>
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, 6(7), e1000097.
- OECD. (2020). Building resilient economies: Strategies for regulatory and operational preparedness. Organisation for Economic Co-operation and Development. <https://www.oecd.org>
- Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide*. Blackwell Publishing.
- Rodin, J. (2014). *The resilience dividend: Being strong in a world where things go wrong*. PublicAffairs.
- Schoemaker, P., Heaton, S., & Teece, D. (2018). Innovation, dynamic capabilities, and resilience: Strategies for uncertainty. *California Management Review*, 60(3), 48–75. <https://doi.org/10.1177/0008125618769460>
- Sheffi, Y. (2015). *The power of resilience: How the best companies manage the unexpected*. MIT Press.
- Taleb, N. N. (2012). *Antifragile: Things that gain from disorder*. Random House.
- 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>
- Teece, D. J., & Pisano, G. (2018). Dynamic capabilities and organizational resilience. *Strategic Entrepreneurship Journal*, 12(1), 1–14. <https://doi.org/10.1002/sej.1270>
- Thompson, L., & Brown, M. (2022). Digital transformation and organizational continuity in turbulent environments. *Information & Management*, 59(5), 103637. <https://doi.org/10.1016/j.im.2022.103637>
- 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.
- Walker, A., & Davidson, P. (2023). Developing and measuring organizational resilience: A cross-industry study. *Journal of Business Research*, 160, 113958. <https://doi.org/10.1016/j.jbusres.2023.113958>
- Wilson, A. (2020). Regulatory compliance and resilience in global supply chains. *International Journal of Production Economics*, 227, 107648. <https://doi.org/10.1016/j.ijpe.2020.107648>
- World Economic Forum. (2023). *Global risk and resilience framework*. <https://www.weforum.org>
- You, T., Chen, H., & Wang, L. (2023). Digital infrastructure and organizational resilience during crises. *Technological Forecasting and Social Change*, 191, 122478.
- Yu, W., Jacobs, M., & Chavez, R. (2021). Supply chain resilience in the COVID-19 pandemic: Evidence from multiple industries. *International Journal of Operations & Production Management*, 41(3), 299–321. <https://doi.org/10.1108/IJOPM-05-2020-0300>
- Yuanxing, L., Li, Y., & Zhang, Z. (2024). Organizational resilience in highly regulated industries. *Journal of Business Research*, 178, 113645. <https://doi.org/10.1016/j.jbusres.2024.113645>