Organizational Resilience in the Digital Age: Business Continuity Management Practices Across Croatian Public and Private Sectors

Ante Vuletić
University of Zagreb, Faculty of Economics & Business, Croatia

Abstract

Digital transformation is reshaping organizational risk and exposing gaps in business continuity management (BCM). This paper presents a mixed-methods study of 80 private and public Croatian organizations conducted from March to July 2025. Using questionnaires and interviews with 16 senior managers, it examines BCM maturity and sector differences. The key finding is clear: 58% of private organizations have fully implemented BCM, compared with 32% in the public sector. Private firms adopt BCM changes 43% faster and use cloud backup and automation about twice as often. Organizations that integrate digital technology into BCM achieve 40% stronger crisis response. COVID-19 marked a turning point, with three-quarters of organizations expanding BCM after 2020. The study highlights top management support and regular stress testing as the strongest predictors of success within Croatia's evolving EU regulatory environment, including the NIS2 Directive.

Keywords: business continuity management; digital transformation; public sector; private sector; organizational resilience

Paper type: Preliminary research

Received: Jan 8, 2026
Accepted: Apr 2, 2026

DOI: 10.2478/crdj-2026-0005

Introduction

March 2020 was, for many Croatian organizations, a kind of forced audit. Almost overnight, the pandemic stripped away the assumption that disruption would be temporary, localized, and manageable with existing procedures. Some organizations held up. Others, and this came up repeatedly in the interviews I conducted for this research, had no plan to fall back on. One public-sector manager I spoke with described the early weeks of the lockdown as "improvisation from the top down." That phrase stuck with me, because improvisation is precisely what business continuity management is supposed to prevent.

The pandemic did not invent organizational vulnerability, of course. What it did was make visible a set of structural weaknesses that had been quietly accumulating for years, partly because of how rapidly digital technologies had been embedded into core operations without a corresponding investment in resilience, and partly because BCM had never quite escaped its reputation as a compliance exercise rather than a genuine strategic priority. Cyberattacks were already growing more sophisticated before COVID-19. Cloud infrastructure was already changing the geography of organizational risk. The pandemic compressed the timeline for confronting these pressures. In this sense, digital transformation should not be viewed only as a source of new vulnerabilities, but also as a potential driver of organizational excellence and resilience when implemented systematically (Savastano et al., 2022).

Croatia's situation is worth examining, not just as a proxy for broader European trends. Since joining the EU in 2013, the country has been navigating a dual transformation: adapting to EU regulatory frameworks while simultaneously digitizing an economy that, in some sectors, still carries significant legacy infrastructure. The NIS2 Directive, which entered into force across the EU in 2023 and required national transposition by October 2024, has sharpened the stakes considerably, particularly for public sector organizations, which now face mandatory cybersecurity and resilience requirements that go well beyond what most currently have in place (European Union, 2023).

Three questions structure this study: What separates public and private sector organizations in terms of BCM maturity, and is the gap as large as practitioners tend to assume? How has digital transformation changed the way Croatian organizations think about and implement continuity planning? What distinguishes organizations that have genuinely succeeded at BCM from those that have stalled or never meaningfully begun? Addressing these questions, the study contributes to the literature by conceptually linking business continuity management maturity with digital transformation as an organizational capability and by providing comparative empirical evidence on sectoral differences in a Central and Eastern European context.

Theoretical Framework

It is worth briefly tracing how BCM has arrived at where it is today, because the discipline's history helps explain some of the gaps this study uncovers. The field emerged from IT disaster recovery in the 1970s and 1980s, a fairly narrow set of concerns about what happened to data and systems when something went wrong. For a long time, "business continuity" was essentially an IT department problem, something that lived in server rooms and backup tapes. The idea that it should be a board-level strategic concern is, historically speaking, quite recent.

ISO 22301, first published in 2012 and revised in 2019, was a significant step in broadening that scope. The standard defines BCM as a holistic management process encompassing risk assessment, business impact analysis, strategy formulation, plan implementation, and ongoing testing within a continuous improvement cycle (ISO 22301:2019). Certification against ISO 22301 has become a meaningful signal of organizational maturity, not just technical competence. That said, as the data in this study show, certification rates in Croatia remain low, raising questions about whether the standard has genuinely penetrated organizational culture or is mostly aspirational for most organizations.

Digital transformation has complicated the BCM picture in ways that are still being worked out in the literature. Recent research suggests that digital transformation should not be understood only as a technological shift, but also as an organizational capability that can support sustainable business excellence in turbulent environments (Savastano et al., 2022). From a BCM perspective, this implies that digital transformation can strengthen resilience when aligned with continuity planning, governance, and adaptive organizational processes.

The paradox that Herbane (2019) identifies is real: the same technologies that make organizations more capable also make them more fragile. Recent research also suggests that digital transformation, when strategically aligned with organizational processes and governance, can strengthen broader dimensions of business excellence and resilience in turbulent environments (Savastano et al., 2022). A single compromised credential can now cascade into a system-wide breach in ways that were not possible when critical processes ran on isolated, on-premises systems. Cloud infrastructure introduces geographic redundancy and scalability, genuine resilience benefits, but it also creates new single points of failure, particularly when organizations are heavily dependent on a small number of providers. The 2021 Fastly outage, which took down large portions of the internet for several hours, was a vivid illustration of this.

Engemann and Henderson (2021) argue that cybersecurity and BCM, which were developed as separate disciplines, can no longer be treated as separate disciplines. An organization that has excellent backup and recovery procedures but no coherent response to a ransomware attack has a BCM program with a significant blind spot. Crask (2024) pushes this further, exploring how AI and machine learning can enhance real-time threat detection and decision support during crises, though he also notes, with appropriate caution, that AI systems themselves introduce new dependencies that BCM programs need to account for.

The public-private divide in BCM has attracted growing research attention. The differences are not just about money, though resources matter. They are about incentive structures, decision-making processes, and what organizations are ultimately accountable for. Private sector firms face market consequences for disruptions, lost revenue, reputational damage, and competitive disadvantage that create fairly direct pressure to invest in resilience. Public sector organizations face a different accountability structure. Service disruptions cause public frustration and political pressure, but the feedback loop is slower and less precise. This, combined with procedural constraints, institutional rigidities, and slower decision cycles often associated with public-sector digital transformation, goes a long way toward explaining the patterns that emerge in this study (Mergel et al., 2019).

Wallace and Webber (2018) observed that private-sector organizations were more likely to integrate BCM into strategic planning, treating it as a competitive capability rather than a compliance requirement. Gibb and Buchanan (2020) found that public sector organizations often struggle to prioritize BCM against more immediate service delivery demands. Spremić et al. (2022) add a specifically Croatian dimension, noting that legacy systems, skills gaps, and organizational resistance to change compound the challenges that public institutions face in digital transformation more broadly. Post-pandemic, Ponomarov and Holcomb (2025) argue that the resilience literature needs to move beyond localized disruption scenarios toward frameworks that can accommodate systemic, prolonged crises, precisely the kind of scenario that COVID-19 represented.

Research Framework

The research design combines quantitative survey data with qualitative interviews, a pairing that proved more illuminating than either method alone. Numbers tell you what; people tell you why.

Data

Between March and July 2025, data were collected from 80 Croatian organizations: 40 from the public sector and 40 from the private sector. The public sector sample included government ministries, regional and local authorities, public utilities, healthcare institutions, and higher education institutions. On the private side, I aimed for sectoral diversity, with financial services, telecommunications, manufacturing, retail, and professional services represented, and a mix of large enterprises and mid-sized firms. All participating organizations had at least 100 employees and had been operating for at least 3 years, criteria intended to ensure that BCM was at least theoretically within organizational reach.

The sample was constructed using purposive sampling to ensure representation of organizations with sufficient structural complexity for BCM implementation. The inclusion criteria (minimum number of employees and operational maturity) were defined to capture organizations in which continuity planning is both relevant and feasible. While the sample is not statistically representative of the entire Croatian economy, it reflects a deliberate balance between public and private sector entities, as well as diversity across industries and organizational types. This approach supports meaningful sectoral comparison while maintaining analytical depth in the interpretation of BCM practices.

All 80 organizations completed a structured questionnaire built around the ISO 22301 framework. The instrument assessed six BCM components: formal policy, risk assessment, business impact analysis, continuity strategies, testing programs, and certification status. It also captured data on digital technology adoption within BCM contexts (cloud computing, process automation, AI-enabled monitoring) and on organizational characteristics and COVID-19 experiences. To give depth to the survey findings, I conducted semi-structured interviews with 16 senior managers (eight per sector) holding titles such as Chief Information Officer, Risk Manager, or Business Continuity Manager. These conversations, which ran 60 to 90 minutes each, were where the real texture of BCM practice emerged: the procurement delays, the leadership battles, the near-misses during COVID-19 that nobody had written up in a formal report.

Research Methodology

BCM maturity was operationalized as a composite index across the six ISO 22301 components, scored on a standardized scale. Each BCM component was measured using multiple indicators reflecting the presence and depth of implementation (e.g., formalization, documentation, and operational use). Scores were aggregated into a composite index to capture overall BCM maturity, with equal weighting assigned to each component in line with the integrated structure of the ISO 22301 framework. The use of a standardized scoring approach enabled consistent comparisons across organizations while preserving the multidimensional nature of BCM as both a strategic and operational capability. Quantitative analysis involved descriptive statistics, independent-samples t-tests for sectoral comparisons, and multiple regression to identify predictors of implementation success. Effect sizes were calculated alongside significance tests, given the sample size.

To ensure methodological robustness, several steps were taken to enhance the validity and reliability of the research design. The survey instrument was grounded in the ISO 22301 framework, thereby providing content validity by aligning the measurement items with established BCM dimensions. Internal consistency was assessed across the six components, and the composite index was constructed using standardized scoring to ensure comparability across organizations. Although the sample size limits the generalizability of the findings, the balanced representation of public and private sector organizations strengthens the internal validity of sectoral comparisons. In addition, the use of a mixed-methods approach enabled triangulation between quantitative and qualitative data, increasing the credibility of the results. Nevertheless, the study is subject to potential self-reporting bias and reflects a cross-sectional snapshot of BCM practices, which should be considered when interpreting the findings.

Interview transcripts were analyzed thematically, following the six-phase approach of Braun and Clarke (2006). Codes were developed inductively from the transcripts — I deliberately avoided imposing a predetermined coding framework — and then organized into themes through iterative review. Where quantitative and qualitative findings converged, I treated this as corroboration; where they diverged, I tried to understand why. That triangulation process shaped several of the interpretations in the discussion section.

Results

BCM Implementation Status

Across the full sample, 42% of organizations have fully implemented BCM systems, 38% have partial implementations, and 20% have no formal BCM at all. Those aggregate figures, though, obscure the sectoral story. In the private sector, 58% of organizations have achieved full implementation. In the public sector, the figure is 32%. A 26-percentage-point gap is not a rounding error — it reflects genuinely different organizational realities.

ISO 22301 certification tells a similar story, but with even sharper contrasts. Overall, 18% of organizations hold current certification, and another 26% are in the process of obtaining it. By sector, 28% of private organizations are certified, compared with 8% of public ones. This matters because certified organizations perform measurably better — their recovery times are 40% shorter, and they score 2.3 times higher on crisis preparedness assessments. Whether certification causes better performance or whether it is a proxy for the kind of organizational commitment that produces better performance is a question the data cannot fully resolve, but the association is robust.

Table 1 BCM Component Implementation by Sector

BCM Component	Public Sector (%)	Private Sector (%)
Formal BCM Policy	68	81
Risk Assessment	54	73
Business Impact Analysis	46	76
Continuity Strategies	49	68
Testing Programs	31	47
ISO 22301 Certification	8	28

Source: Author's own research (2025)

The component-level breakdown in Table 1 is worth examining carefully. The gap in business impact analysis —46% versus 76%, a 30-percentage-point difference—is particularly striking. BIA is foundational: without it, organizations do not know which processes are truly critical, leaving their continuity strategies essentially guesswork. The testing gap (31% versus 47%) is also significant because testing is where plans get validated or exposed as inadequate. Several public sector interviewees acknowledged that their organizations had BCM documents that had never been tested in any meaningful way. "We have a binder," one manager told me. "I am not sure anyone has opened it since 2019."

Digital Technology Adoption

Cloud-based backup and recovery is now the norm in the private sector: 67% of private organizations use it, compared to 41% in the public sector. Process automation within BCM contexts shows an even wider gap of 45% versus 23%. These are not just technology preferences; they have direct operational consequences. Organizations that have integrated digital tools into their BCM frameworks report crisis response capabilities that are, on average, 40% stronger than those relying on manual processes. Recovery time, coordination speed, and decision-making clarity all improve.

COVID-19 accelerated adoption across both sectors. By the time I was collecting data in 2025, 78% of organizations had expanded or overhauled their BCM programs since 2020. However, the pace of that change varied: private-sector organizations implemented BCM modifications 43% faster than their public-sector counterparts. Some of that speed advantage reflects genuine agility; some of it reflects the absence of procurement constraints that can turn a straightforward technology purchase into a multi-year approval process.

Success Factors and Barriers

The regression analysis points clearly to top management support as the dominant predictor of BCM success. Organizations with active executive sponsorship are 2.1 times more likely to achieve full implementation than those where BCM has been delegated without leadership engagement. This finding is consistent across both sectors, though its implications differ. In the private sector, executive engagement often comes from a commercial calculation; a major disruption is expensive and reputationally damaging. In the public sector, it tends to depend more on individual leadership styles, making it less predictable and less durable.

Regular testing is the second major predictor. Organizations that run BCM exercises at least twice a year show 67% greater success when an actual crisis occurs. This is not surprising: you get better at things you practice. However, the testing rates in this sample suggest that many organizations treat their BCM plans as documents rather than capabilities. One private-sector CIO described running a full-scale simulated ransomware response exercise and discovering that the incident command structure listed in the plan included two people who had left the company. "That is the kind of thing you only find out by actually doing the exercise," he said.

The barriers differ by sector in instructive ways. Public sector organizations pointed overwhelmingly to bureaucracy (86%), funding constraints (84%), and skills gaps (73%). The bureaucracy issue came up in almost every public sector interview, and not in an abstract way; people described specific procurement processes that took 18 months, budget cycles that required planning for technology investments three years in advance, and hiring procedures that made it nearly impossible to recruit specialized cybersecurity or BCM expertise. Private-sector challenges were real but distinct in character: rapid technological change (52%), market pressure (47%), and cost-optimization requirements (41%). The private sector tension is essentially about competing priorities, not structural barriers.

Performance Outcomes

The performance data are consistent with the implementation data. Organizations with mature BCM systems identify threats 45% faster, coordinate crisis responses 28% more effectively, and reach critical decisions 33% more quickly. Private sector organizations outperform public sector organizations on all three metrics, which aligns with higher BCM maturity scores. What is perhaps most interesting is the compounding dynamic: organizations that invested early in BCM are now better positioned to absorb the next round of digital transformation, because they have the organizational muscle memory to integrate new technologies into resilience frameworks rather than treating them as separate concerns.

Discussion

The findings of this study provide a structured explanation for the observed gap in BCM maturity between public and private sector organizations in Croatia. While the descriptive results clearly indicate higher levels of implementation in the private sector, the underlying mechanisms appear rooted in differences in institutional context rather than in managerial awareness alone. In line with the arguments of Mergel et al. (2019), public sector organizations operate within more rigid procedural and governance frameworks, which constrain the speed and flexibility required for effective digital transformation and, by extension, BCM development.

The role of digital transformation emerges as more nuanced than a simple enabler of resilience. Consistent with Savastano et al. (2022), the results suggest that digital technologies contribute to organizational resilience only when they are embedded within broader managerial and strategic frameworks. Organizations that adopt cloud infrastructure, automation, and monitoring tools without aligning them with continuity planning do not achieve the same performance gains. This supports the view that digital transformation should be conceptualized as an organizational capability rather than a purely technological shift.

The strong effect of top management support identified in this study reinforces a well-established but often under-implemented principle in the BCM literature: continuity cannot be entirely delegated to technical or operational units. As indicated by Engemann and Henderson (2011), BCM maturity depends on leadership commitment and integration into strategic decision-making processes. The 2.1-fold difference in implementation likelihood observed in this study illustrates how leadership engagement translates directly into organizational outcomes.

The importance of regular testing further highlights the distinction between formal compliance and functional capability. Organizations that conduct frequent stress testing demonstrate significantly better crisis response performance, suggesting that BCM effectiveness is driven not only by the existence of plans but by their continuous validation and adaptation. This finding aligns with prior research that emphasizes the operational dimension of resilience as a dynamic, practice-based capability rather than a static organizational attribute.

Finally, the results point to a compounding effect between early investment in BCM and the ability to manage ongoing digital transformation. Organizations that developed continuity capabilities prior to major disruptions such as COVID-19 appear better equipped to integrate new technologies into their resilience frameworks. This supports the argument that organizational resilience is path-dependent, shaped by prior investments, learning processes, and institutional readiness, rather than being easily constructed in response to crisis alone.

Conclusion

What this study ultimately shows is that BCM maturity in Croatia is unevenly distributed in ways that are both predictable and consequential. The private sector leads not because private-sector managers are more farsighted, but because the incentive structures and organizational conditions that support BCM investment are more consistently in place. The public sector lags, not because public servants do not understand the importance of resilience, but because the structural conditions that would enable BCM development (agile procurement, competitive hiring, flexible budgeting) are largely absent.

Several things seem clear from the data. BCM is not a technical problem with a technical solution; it is an organizational challenge that requires sustained leadership attention. The 2.1x implementation advantage that executive-sponsored organizations enjoy cannot be replicated by buying better software. Regular testing is non-negotiable; a BCM plan that has not been stress-tested is a liability, not an asset. Moreover, digital transformation and continuity planning must be developed together; organizations that treat them as separate workstreams end up with brittle digital capabilities and obsolete continuity plans.

For Croatian public-sector organizations, the NIS2 Directive creates both pressure and opportunities. The pressure is obvious: mandatory cybersecurity and resilience requirements that many public bodies are not currently meeting. The opportunity is that NIS2 provides a legitimate external mandate that BCM advocates within public organizations can use to make the case for investment and structural reform. Policymakers should take seriously the procurement and hiring constraints that interviewees identified; these are not complaints about bureaucracy for its own sake, they are structural barriers to organizational resilience that regulation alone cannot fix.

There are things this study cannot tell us. The cross-sectional design captures a moment in time; longitudinal data would be needed to track whether the post-COVID BCM expansion has been sustained or whether organizations have drifted back toward pre-pandemic complacency. The sample, though carefully constructed, is limited to Croatian organizations, and comparative data from other Central and Eastern European EU member states would help situate these findings. The role of AI in BCM, both as an enabling technology and as a new source of organizational dependency, deserves dedicated investigation as adoption accelerates. These are the directions I would point future research toward.

The organizations in this study that have built genuine BCM capability share one characteristic above all others: they started before they needed it. The ones still catching up in both sectors mostly started because a crisis forced them to. That asymmetry between organizations that invest in resilience proactively and those that wait for disruption to motivate them is probably the most important finding in this paper, and the hardest to act on.

From a policy perspective, these findings suggest that regulatory frameworks, such as the NIS2 Directive, should be complemented by institutional reforms to address structural barriers to BCM implementation, particularly in the public sector. Without improvements in procurement flexibility, talent acquisition, and organizational agility, compliance-driven approaches risk producing formal alignment without substantive resilience. Strengthening organizational resilience, therefore, requires not only regulatory pressure but also systemic capacity-building across public institutions.

References

1. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
2. Crask, J. (2024). *Business continuity management: A practical guide to organizational resilience and ISO 22301*. Kogan Page.
3. Engemann, K. J., & Henderson, D. M. (2011). *Business continuity and risk management: Essentials of organizational resilience*. Rothstein Associates.
4. European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. *Official Journal of the European Union, L 333*, 80–152.
5. Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management, 26*(2), 128–141. https://doi.org/10.1016/j.ijinfomgt.2005.11.008
6. Herbane, B. (2019). Rethinking organizational resilience and strategic renewal in SMEs. *Entrepreneurship & Regional Development, 31*(5–6), 476–495. https://doi.org/10.1080/08985626.2018.1541594
7. International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. ISO.

8. Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly, 36*(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002

9. Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management, 20*(1), 124–143. https://doi.org/10.1108/09574090910954873

10. Savastano, M., Zentner, H., Spremić, M., & Cucari, N. (2022). Assessing the relationship between digital transformation and sustainable business excellence in a turbulent scenario. Total quality management & business excellence, 1-22. https://doi.org/10.1080/14783363.2022.2063717

11. Spremić, M., Zentner, H., & Zentner, R. (2022). Measuring digital business models maturity: Theory, framework, and empirical validation. IEEE transactions on engineering management, 71, 6553-6567. https://doi.org/10.1109/TEM.2022.3226864

12. Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science, 89*, 201–218. https://doi.org/10.1016/j.ssci.2016.06.015

13. Wallace, M., & Webber, L. (2010). *The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets* (2nd ed.). AMACOM.

14. Zsidisin, G. A., & Henke, M. (Eds.). (2019). *Revisiting supply chain risk*. Springer. https://doi.org/10.1007/978-3-030-03813-7

About the Author

Ante Vuletić is an Associate Professor at the Faculty of Economics & Business, University of Zagreb, where he teaches courses on Business continuity and Artificial intelligence. His research sits at the intersection of technology adoption and organizational resilience — he is particularly interested in why some organizations build genuine continuity capability while others produce plans that never survive contact with an actual crisis. He holds a Ph.D. in Business Economics from the University of Zagreb and consults for public sector organizations on resilience and continuity planning. The author can be contacted at **avuletic2@net.efzg.hr**.