International Journal of Accounting and Economics Studies, 12 (7) (2025) 346-352

International Journal of Accounting and Economics Studies

Website: www.sciencepubco.com/index.php/IJAES
https://doi.org/10.14419/4189zh28
Research paper

The Impact of Digital Transformation on Business Continuity Management: Redefining Corporate Strategies for Resilience

Haslinda Binti Musa [1] *, Surya Seetharaman [2]

[1] Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka
[2] Saveetha School of Law, Simats and SP Jain School of Global Management
**Corresponding author E-mail: haslindamusa@utem.edu.my*

Received: August 1, 2025, Accepted: October 14, 2025, Published: November 9, 2025

Abstract

The digital revolution is also contributing to the disruption of Business Continuity Management (BCM) by leading to the shifting of technology in organizational structures. This offers new avenues to organizations on how they can improve their resilience improvement strategies.. In the face of digital disruption, organizations are not simply challenged by digital transformation, but also by volatile market conditions and geopolitical uncertainties. Therefore, planners with BCM responsibilities are weighed down by multi-faceted issues in assessing how best to continue operations and be prosperous in the long-term by including digitization in the BCM planning. This paper will identify key trends and case studies on the use of digital technologies (e.g., AI, cloud, workplace analytics, etc.) to identify risks, shape response, and help assess recovery IT during crises. The results illustrate how organizations with a digital transformation agenda show more resilience and preparedness to anticipate digital disruptions; reorganize communications flow; and mobilize their resources in response to challenges. Moreover, the paper identifies the criticality of fostering organizational cultural change, characterized by agility, innovation, digital transformation, and collaboration. By adopting digital innovation concepts, organizations can enhance their contingency planning and develop a more effective response to unforeseen events. Additionally, organizations will redefine and have the capacity to move beyond their approach to continuity planning, as they find that not only can they emerge through disruption, but they can also emerge with a greater resilience and competitive edge in an environment that is becoming increasingly volatile and uncertain. The study adopts a mixed-methods approach, combining a structured survey of 120 professionals with 10 semi-structured interviews, to examine the integration of digital tools in BCM practices. This paper offers insights for corporate individuals seeking to harness digital innovations to bolster their resilience and sustainability strategies in the future, to strengthen long-term organizational resilience.

Keywords: *Digital Transformation; Business Continuity Management; Resilience; Corporate Strategies; Artificial Intelligence; Cloud Computing; Data Analytics; Organizational Agility; Risk Management; Crisis Response.*

1. Introduction

BCM has transitioned from a passive approach of reducing risk to a proactive approach. The external need to adapt to an increasingly uncertain global environment caused this change. The current crisis, such as COVID-19 and rapid disruptions of operations due to technology, has contributed to this shift to a great extent. (Aggarwal, 2024). The digital transformation agenda is at the heart of developing BCM out of a risk mitigation strategy into a modern-day, strategic business imperative (Cardoso et al., 2025). The drive to rapidly introduce digital technologies into a business, such as artificial intelligence (AI), cloud, big data, Internet of Things (IoT), and automation, into everyday business operations. These digitalisation methods help to drive efficiency but also set the foundation for many organisations to build resilience whilst supporting continuity long-term (George et al., 2020). Disruptions in today's world have become commonplace and are no longer rare phenomena, as operations are relying on connectivity through digital platforms to conduct business. The pandemic's disruption to business operations underscored that traditional views of virtuality and static BCM processes were insufficient to provide organisations with the functionality they needed, even with the most robust plans (Browder et al., 2023). Examples in studies such as Deloitte (2021) highlighted that mature digitalised BCM ascribed to aspects of business, better promoted rapid recovery in the most stressful situations compared to organisations that had less developed BCM practices. Integrating technology through digitalisation into BCM is imperative if organisations wish to sustain and promote ongoing competitive advantages in an unpredictable world order (Ciampi et al., 2022). The aspect of digitalisation of processes enables the ability to mitigate risk, based on real-time monitoring, scenario modelling, and automated recovery. Each of these elements enables reduced latency and human error response during crisis times (Alsaidi & Shehab, 2022).

AI-enabled systems support the identification of early signals of disruption and enable the selection of mitigation strategies, while cloud providers allow critical data to be accessed at all times, even when physical premises are shut down (Chakravorti, 2023). In addition, these technologies enable organizations to deploy data-driven decision-making and agility, which is an essential component of resilience (Elgazzar et al., 2021). Organizational resilience requires robust digital structures, especially in a world of remote and hybrid working, whereby digital capability helps support real-time virtual operations, secure communications, and remote or distributed teams (Reddy & Sampath, 2024). All of these technologies are fantastic, but simply embracing them will not achieve effective digital transformation of BCM; a cultural shift in organizational behavior is required. Company leaders must prioritize agility, collaborative decision-making, and continuous innovation. Furthermore, partner organizations must navigate inter-dependencies, address cybersecurity, data governance, and regulatory compliance as digital continuity plans, which frequently involve processing the collection of sensitive personal data across borders (Awad & Martín-Rojas, 2024). Furthermore, movements toward digitization have not happened uniformly across sectors; with advanced sectors such as finance, healthcare, and IT embedding digital BCM at a greater scale than most SMEs that are limited by resource capacity and low digital literacy (World Economic Forum, 2023).

Addressing the digital divide is crucial for bridging resilience across organizations and ensuring resilience can be accessed by ALL, not just those who are digitally confident (Chiarini & Vagnoni, 2020). Organizations that effectively leverage their BCM with digital transformation will gain sustainable competitive advantages, not only during crisis recovery, but as part of a longer-term adaptability strategy. As Chiarini & Vagnoni (2020) noted, digital tools enable organizations to prioritize operational continuity while simultaneously being able to innovate and change in real time, creating a path to sustainable growth in the post-pandemic phase. With increased interest in integrating digital with BCM, and the acknowledgement that the scholarship exists in a platform of fragmentation, there are gaps still existing as to how implementation, situation-dependent industry best practices, and sustained results influence challenges (Breidbach et al., 2024). This piece of research conceptually explores the opportunity for accountability by examining how organizations utilize their digital tools and transportation strategies to ensure continuity. The paper explores the enablers, inhibitors, and outputs of integration, providing much-appreciated learnings for organizational leaders, risk executives, and public policymakers. All in all, the notion of a future in BCM that will not just focus on bouncing back and being digitally resilient, but the idea of bouncing forward with speed and force for the new normal has brought tangible improvements in resilience, operational efficiency, and crisis recovery outcomes.

Organizations are increasingly adopting digital technologies for Business Continuity Management (BCM); however, it is essential to recognize the regulatory environment, specifically data privacy regulations, which will influence organizations' usage of and adoption of digital tools within BCM (Gao & Yu, 2023). Regulatory frameworks such as the General Data Protection Regulation (GDPR) are important because the way that organizations utilize digital solutions to support business continuity is changing as a result of the frameworks (Felder & Prince, 2025). Organizations must be aware of the legal requirements for the handling of sensitive data; therefore, using digital tools in BCM must be consistent with handling personal identity information and comply with data protection legislation, such as the GDPR (Coad & Storey, 2021). If an organization decides to adopt digital tools for BCM, it will have to abide by compliance requirements for handling sensitive data (Breidbach et al., 2024). Laws such as the GDPR impose guidelines that limit how organizations collect, process, and store personal data, which may influence the company's choice of technology (Chakravorti, 2023). Organizations using digital tools in a crisis may have to implement additional controls related to encryption, data masking, or anonymization for compliance while still using digital tools in an emergency (Chakravorti, 2023). These laws will also require organizations to govern data in their BCM plans and take measures to protect themselves from cybersecurity risks (Ellen et al., 2022). Therefore, when organizations address compliance issues related to data privacy laws and adopt digital BCM tools, they can ensure resilience during a crisis while also complying with laws that protect the rights of their customers and employees, as well as meeting the legal requirements for handling sensitive data (Ellström et al., 2021). These are compliance considerations that organizations should think of as they develop digital transformation initiatives, so they can maintain continuity and be responsible in protecting relevant data integrity and personal identity.

2. Literature Review

2.1. Evolution of business continuity management (BCM)

Business Continuity Management (BCM) has historically been a risk management tool that focuses on managing the interruption to essential business activities in connection with a crisis (Motro et al., 2024). BCM was originally established in the context of a set of strategies for disaster recovery and disaster preparedness activities for business functions, focused on IT recovery and recovery of business infrastructure, during the 1980s and 1990s. BCM represents a very different point of view, as BCM has advanced significantly in the last 20 years from a limited view of risk management into a much broader strategic management process with the expressed purpose of assisting the increase in organizational resilience (George et al., 2020). The shift in the understanding of BCM has arisen because of increasing interdependencies in the world supply chain, increased regulatory oversight and compliance, as well as the ensuing obligations to stakeholders in the form of risk management assurance and transparency (Banihashemi et al., 2017). Now that organizations have also recognized that BCM has moved away from being solely a crisis survival mechanism to become an enabler of strategic competition during a crisis, organizations must be resilient before they can compete. The ISO 22301 standard, which details the structure of BCM practice, defines both business continuity and resilience, and suggests that business continuity should be framed in the context of an organization's objectives, leadership, and stakeholder commitment. These changes show that the discussions around resilience are moving towards a full acceptance of it as a critical strategic function.

Recent studies indicate that the implementation of BCM practices tends to look quite different across sectors (Alshamsi, 2024). Financial Institutions and Healthcare Organizations typically operate with mature continuity programs since their services are essential (Alsaidi & Shehab, 2022). SMEs do not have the same resources and competence when trying to use BCM (Li et al., 2024). This is relevant in determining the scalable BCM solutions as an element of organisational size and available resources. The issue of flexible BCM has been fast-tracked in the post-COVID-19 pandemic era. Moreover, their prepared continuity plans helped to shift organizations to remote work without losing productive time as quickly as possible following the disruptions in the supply chain (Akib et al., 2022). The phenomenon of digital transformation in the BCM environment is becoming increasingly relevant. Such BCM tools as predictive analytics, cloud structures, and AI-backed risk evaluation have been leading to the emergence of a more proactive and information-heavy process (Basa, 2024). As an example, most of the tools are already being used to model scenarios faster than the manual method (Awad & Martín-Rojas, 2024). New technologies also provide an opportunity to automate recovery processes and better organize the work of crises (Alsaidi & Shehab, 2022).

2.2. Digital technologies and their role in enhancing BCM

Digital technologies have also revolutionized Business Continuity Management (BCM) by identifying risks, real-time tracking, and automated decisions (Gartner, 2022). The foundation technologies behind the implementation of agile, responsive, and data-driven BCM are artificial intelligence (AI), big data analytics, cloud computing, and IoT (Bhole, 2023). Such a change in technology renders organizations out of the old and industrial method of developing continuity plans and shifting towards one that is dynamic, real-time, and foresees the ability to change plans as events progress due to threats and alterations in circumstances (He et al., 2022). The use of AI is growing in popularity and is increasingly being used alongside predictive models within BCM environments, as organizations leverage not only historical information, but also real-time or current data to forecast an interruption to their business operation. For example, AI tools will allow organizations to pick out abrupt changes in user traffic, which can help identify if a cyberattack is imminent, or process an international news feed that can show potential risks for any interruption to a supply chain (World Economic Forum, 2023). AI tools can decrease an organization's response time or improve the accuracy of a threat analysis that can stem the overall organizational impact of a disruption (Zhou et al., 2021).

Another important enabling technology is cloud computing, which enables access to organizational information and applications from anywhere, allowing for remote work and providing support for the organization's continuity in the event of a physical disruption. Scalability of the cloud-based infrastructures is specifically applicable to SMEs that lack a wide extent of IT resources (Walther et al., 2011). As an example, a 2022 report by Gartner found that over three-quarters of organizations with cloud-based BCM frameworks perceive higher rates of resilience and recover better after the disruptions than those organizations that do not possess cloud-based BCM frameworks. Big data analytics enables the assessment of risks and facilitates real-time decision-making based on the analysis of large data sets across various sources, including social media and IoT sensors, thereby translating into actionable insights that are crucial in crisis moments (World Economic Forum, 2023). Likewise, IoT can also assist in BCM by monitoring and evaluating other hazards in real-time to establish situational awareness of the physical properties of tangible physical assets and the climate conditions and discover warning risks, including temperature variations, building instabilities, and unavailability (Tarigan et al., 2025). When moving forward in favor of companies, organizations that adopt digital BCM tools should also be aware of the consequences they will experience (Warner & Wagner, 2019). The issues surrounding data privacy, cybersecurity risks, and the need for integral integration are among the challenges that organizations must address. This demands a culture of constant learning and innovation because the digital BCM capabilities require the training of employees and change management (Chakravorti, 2023).

2.3. Theoretical contribution to understanding digital transformation in BCM

The two theoretical approaches used in this study are Dynamic Capabilities Theory and Resource-Based View (RBV), aiming to advance the theoretical underpinnings of investigating digital transformation procurement within Business Continuity Management (BCM). Dynamic Capabilities Theory is the term that denotes the ability of the organization to integrate, construct, and adapt external and internal competencies to handle the immediate and continuing evolving conditions (Jabr, 2023). Using the idea of BCM, digital tools and technologies, which include artificial intelligence (AI) and cloud computing, are applied to establish competencies that would support and advance organizational resilience and improvement, allowing the organization to consider faster and more flexible procedures to address potential interruption or a disclosure process more promptly (Hokmabadi et al., 2024). At the conceptual level, dynamic capabilities help one and organizations to comprehend in a better way how they use digital technologies that they can leverage upon, and the surrounding human processes that assist in predicting the upcoming crises, enhancing the recovery strategies, and supporting BCM to eliminate the long-term continuity gap (Huemann & Silvius, 2017). About the RBV, valuable, rare, and inimitable resources and capabilities provide organizations with a sustained competitive advantage. For this study, this research will frame digital transformation as a strategic resource that provides unique capabilities, due to the technologies involved, which enhance the BCM framework and may provide an organization with a strategic advantage (Johri & Olds, 2011). Hence, as these two theoretical perspectives work together, they can enhance the understanding that digital transformation represents not only the specific tools for managing a crisis but also an important issue surrounding the complex aspects of organizational resilience in the long term.

2.4. Gap in literature: balancing digital transformation with security concerns in BCM

The Literature Review provides a robust entry point into the evolution of Business Continuity Management (BCM), highlighting the increasing role of digital technologies, including the adoption of cloud computing and artificial intelligence (Petropoulou et al., 2024). However, one element that has not been critically engaged with in the literature is the balance between the potential opportunities digital tools offer an organization and the higher levels of risk they may bring, particularly regarding cybersecurity risks (Reddy & Sampath, 2024). It is a concern, considering the limited literature that looks critically at the notion of data security, which one contends is one of the more serious concerns facing an organization (Rupeika-Apoga et al., 2022). This produces an important gap in BCM. While digital tools can provide more efficiency and crisis responsiveness, they may build more vulnerability in terms of a cyber-attack (Russpatrick et al., 2021). Organizations are in a constant struggle over digital continuity and their security operations. The literature must also critically address the tensions involved between and amidst digitalisation and security so that organisations can take advantage of digital technologies in BCM but do not do so in violation of their requirements under data protection and cybersecurity (Vial, 2019). Highlighting the gap would enhance the understanding and identification of the tensions between the potential upside and the potential downside risks of digital transformation in BCM.

2.5. Enhancing BCM with digital tools: opportunities and vulnerabilities

The literature review highlights the opportunities that digital tools present for Business Continuity Management (BCM), including enhanced risk identification, improved crisis response, and increased organizational resilience (Weeks et al., 2021). A more detailed analysis of the risks related to the implementation of these tools and technologies could have been presented in the literature review. Despite the numerous positive effects of digital adoption, it would be counterproductive to overlook the associated issues, including data privacy, cybersecurity, and system integration problems (World Economic Forum, 2023). Companies that apply digital tools in BCM must understand that digital transformation is two-way and that, whereas the former can lead to a higher level of crisis management, they are susceptible to new or another type of threat (Warner & Wagner, 2019). A literature review would help to see how organizations manage the exposure to their data and other external assaults on cybersecurity, especially in cases when either the digital tools organizations adopt

in their strategies to deal with BCM become targets of a cyber-attack or their sensitive data betrays them. The association warrants exploration because other organizations embrace the application of such digital solutions in BCM, together with defending their systems against the emerging digital threats (Lezzi et al., 2025).

3. Methodology

3.1. Research design

The study employed a mixed-methods approach, combining qualitative and quantitative methods. The combination of methods used to present the multiple-layered impacts of digital transformation on Business Continuity Management (BCM) proved most effective. In the quantitative part of this study, a structured survey of persons working in information technology and other risk management fields in different industries was deployed. Semi-structured interviews were conducted to provide an in-depth description of organizational practices and strategies in a qualitative aspect of this research.

3.2. Data collection

The primary data collection instrument was an online questionnaire distributed through professional networks and professional forums. The questionnaire consisted of closed-ended and Likert-scale questions aimed at exploring the use of digital technologies in BCM, risk perception, continuity planning, and organizational resilience. The number of responses received was 120. Ten interviews were conducted via video conferencing with senior managers responsible for BCM implementation. The secondary data included peer-reviewed articles, industry reports, and case studies.

3.3. Sampling method

This research used a purposive sampling method, which allowed the research to rely on invitees who had relevant experience or oversight of BCM practices within their organizations. This purposive sampling method ensured that the participants were informed and could provide useful data. The survey targeted enterprises of medium to large size, and the sectors included finance, health, manufacturing, and IT services.

3.4. Data analysis

The quantitative data from the surveys were analyzed with descriptive statistics and correlation analysis using SPSS. Data analysis highlighted trends in the use of digital tools and their potential impacts on business continuity. The qualitative data from interviews were transcribed and thematically analyzed to identify overlapping themes and strategic insights. The integrated analysis provided a rich overview of contemporary practices and challenges concerning digital BCM operationalization.

4. Results and Analysis

Table 1: Usage of Digital Technologies in BCM Across Industries

Technology	Finance	Healthcare	Manufacturing	IT Services
Cloud Computing	85%	78%	65%	92%
Artificial Intelligence	70%	60%	55%	88%
Big Data Analytics	72%	68%	59%	84%
IoT	45%	52%	69%	58%

Table 1 data shows a strong trend towards the adoption of digital tools across sectors, with IT Services leading the way in usage of cloud (92%) and AI (88%). The finance sector also demonstrated high usage, primarily in cloud and analytics. Manufacturers were lower in AI adoption, but led the way in the usage of IoT tools (69%), emphasising their focus on monitoring physical assets. The healthcare sector demonstrated a balanced adoption rate, offering policies that utilized digital tools to maintain continuity and care for patients during interruptions.

Table 2: Impact of Digital Tools on Business Continuity Outcomes

Outcome	Improved (%)	No (%)	Worsened (%)	Not Applicable (%)
Response Time to Crisis	78%	18%	2%	2%
Operational Downtime	72%	20%	5%	3%
Employee Communication	80%	15%	3%	2%
Customer Service Continuity	74%	19%	4%	3%

Illustrated in Table 2, digital tools are said to contribute greatly to improved business continuity outcomes and metrics. For example, 78% of respondents have reported improved crisis response time, and 80% of respondents reported improved employee communications. Additionally, the very small ratio of respondents seeing worse outcomes suggests that implementing one digital tool will be an extremely effective means of improving organizational resilience.

Table 3: Challenges in Implementing Digital BCM

Challenge	Frequency (%)	Severity Rating (1-5)	Common Sector
Lack of Digital Skills	64%	4.2	Manufacturing
Cybersecurity Concerns	70%	4.6	Finance
Integration Complexity	58%	4	Healthcare
Budget Constraints	62%	4.3	SMEs

The results in Table 3 indicate which barriers to digital BCM adoption were the most prevalent. The concerns of cybersecurity and a lack of digital skills were referenced the most, with severity ratings of 4.6 and 4.2, respectively. The severity of these findings underscores the importance of investing in cybersecurity infrastructure and upskilling digitally, particularly in sectors such as financial services and manufacturing.

4.1. Sectoral challenges in digital transformation for SMEs

In the outcomes and analysis section, one should discuss the various challenges that Business Continuity Management (BCM) Small and Medium Enterprises (SMEs) encounter when utilizing digital tools. Though big organisations have used and combined digital technologies in a way that leads to the enhancement of BCM, SMEs are still struggling to exploit digital technologies to enhance their resilience adequately (Tarigan et al., 2025). Their major problem is resources. Frequently, SMEs lack the funding to apply the digital technologies that are needed to facilitate suitable BCM (Steen et al., 2023). There is a bigger problem as well: SMEs have a significant digital skills gap, and it is absurd, to say the least, to learn and implement cloud computing or AI (Sagala & Őri, 2024). Infrastructure is also lacking, as evidenced by the fact that in some developing regions, the internet is unreliable, limited, or nonexistent, and there is minimal technology support in the area. The result of these barriers is not only a delayed or imperfect digital transformation, but it also adds vulnerabilities of SMEs in the case of crises (Saeed et al., 2023). According to the findings, there are some industries (manufacturing and health care included) that performed better in terms of adopting the digital tools in their resolve to establish digital integration; however, there is still a definite number of challenges SMEs are left with.

5. Discussion

Results of this research have shown that the use of digital tools has a positive effect on Business Continuity Management (BCM) in terms of improvement of the response to the crisis, communication, and efficiency of operations. The authors highlight AI, cloud computing, and big data analytics as some of the main contributors to resilience since they allow an organization to predict disruptions and streamline recovery measures (Rivera et al., 2021). According to the study, digital technologies enable organizations to respond to the crisis at a higher rate and in a more efficient manner, with digital upskilling and cross-functional governance being the key areas in the support of BCM initiatives (Runner et al., 2024). Consequently, companies implementing such measures are capable of enhancing resiliency to business downturns (Nasiri et al., 2021). Nevertheless, risks, such as cybersecurity issues, a lack of resources, and the disconnect between larger organizations and small-to-medium enterprises (SMEs), continue to present substantial risks (Zhou et al., 2021). The project demonstrates a strong relationship between digital transformation and increased BCM capacity. The use of technologies like AI, cloud computing, big data analytics, or IoT has transformed the ways organizations face the challenges of disruption (Zhang et al., 2018).

Interestingly, business continuity applications cloud solutions are a necessity, particularly in IT and finance industries, enabling flexibility and less reliance on physical infrastructure, which is a highly desirable quality when fighting a crisis such as the COVID-19 pandemic (Zhang et al., 2021). There is an increment in the application of AI tools in real-time threat detection and predictive analytics to assist in detecting risks and responding proactively to organizations (Zhou et al., 2021). The aspects of early detection, role simulation of crisis scenarios, and resource optimization capabilities are also enhancing continuity operations through AI (Zhang et al., 2022). There is also a significant difference in the use of digital tools by different sectors. Another example is that manufacturing organizations are less stringent than other sectors in adopting AI, but they are more advanced in implementing IoT devices to monitor and manage assets (Yu et al., 2011). The emphasis on physical monitoring can also prevent such incidents, as it can preempt failures by keeping them under observation (Alsaidi & Shehab, 2022). The healthcare sector strikes the right balance between the necessity of operational continuity and data privacy. This indicates that implementation of BCM strategies in various sectors would have to be done in a manner that assesses the needs of specific industries according to their operational conditions and compliance issues (Yaşar et al., 2006). Along with the advantages, the study presents a few barriers to the effective application of digital BCM. Cybersecurity, digital capability deficiencies, and funding limitations are the primary barriers, particularly in the finance sector, where there is a significant concern over data security breaches and cloud security vulnerabilities (Zhang et al., 2025). The digital skills gap is currently a major issue in SMEs and traditional sectors, where digital literacy is not yet a mature concept (Reddy & Sampath, 2024). Another aspect that is missing in many organizations is the lack of a consolidated digital culture, which is necessary for constant learning and innovation (Liu et al., 2023). Additionally, digital transformation must be coordinated across IT, risk management, and leadership to ensure that digital tools are integrated into a complex BCM framework.

Nevertheless, more than 70 percent of the respondents mentioned improved crisis response, downtime during operations, and their communication capabilities, which is also consistent with what Deloitte (2021) concludes regarding more agile and better-prepared digitally mature organizations to overcome disruption. Digital BCM is essential to assist companies as it enables them to not only survive the crises but also gain a competitive edge due to real-time insights, decentralized operations, and automated reaction (Rivera et al., 2021). This adaptive strength is especially relevant in the current highly dangerous risk landscape, which involves such global risks as climate change, pandemics, and cyber war(World Economic Forum, 2023). To maximize the benefits of digital BCM, the study suggests several key actions: investing in digital upskilling, establishing cross-functional governance teams, and focusing on ongoing measurement and auditing of digital BCM outcomes. These steps will help ensure that organizations continue to adapt and improve their BCM strategies in the digital age.

6. Practical Implications

The study offers several actionable insights for practitioners. First, organizations should prioritize investments in digital tools that align with their operational risks and continuity goals. Tools such as AI for predictive modeling, cloud computing for remote access, and IoT for real-time monitoring can significantly improve resilience. Second, leadership must address skill gaps by initiating digital upskilling programs for both IT and risk management teams. The suggestions point to exploring policy implications in greater detail in the Practical and Policy Implications section, especially how governments, or industry bodies, can assist in helping SMEs adopt digital Business Continuity Management (BCM), and how they can provide guidance on compliance with regulations concerning cybersecurity. This section of the paper is suitable for expanding on policy implications, as it connects to practical recommendations already discussed above, such as digital-skilling and advising on how to establish a cross-functional team to govern. Similar to the previous section on practical recommendations, one could provide additional elaboration on how national or regional policy-makers could work to support digital transformation through financial incentives, training initiatives, or cybersecurity methodologies for SMEs. Governments and industry bodies could play a crucial part in developing guidelines or

standards on how to adopt secure digital BCM, so SMEs do not fall behind in the digital transition. It would also provide additional depth and related policy implications if one examined regulations regarding cybersecurity. Again, by considering how national or regional regulatory frameworks, for example, GDPR, or regulations regarding cybersecurity, may relate to adopting digital tools in BCM, this practical example would provide policy-makers with insights into possible approaches to help organizations mitigate risks while improving business continuity.

7. Conclusion

In conclusion, this research underscores the transformative role of digital technologies in redefining Business Continuity Management. The integration of AI, cloud systems, and analytics tools allows organizations to anticipate and respond to crises more effectively than ever before. This study emphasizes how digital transformation is reshaping Business Continuity Management (BCM) practices. The findings highlighted how AI, cloud technology, and big data analytics have great value in improving organizational resilience and crisis response. In terms of practical implications, the findings highlighted the correspondence between upskilling and supporting governance arrangements for businesses to take full advantage of digital tools for their BCM strategies. In addition, this study highlighted the qualitative benefits of adopting digital tools, while still noting the cybersecurity threats posed by digital tools, the resource burdens of research, and SMEs will continue to be challenged by their ability to adopt digital BCM strategies fully. The policy implications discussed in the study provide further opportunities for governments and industry bodies to facilitate SME adoption of digital BCM tools, including by developing cybersecurity regulations and facilitating relevant funding and AMC training programs. Future initiatives should be designed with phased implementation plans and supported by longitudinal research to measure their long-term impact. Future research should focus on SMEs to assess the scalability of digital solutions and the long-term implications of AI and machine learning in BCM. Additionally, exploring the intersection of digital transformation and organizational resilience through the lens of Dynamic Capabilities Theory can offer deeper insights into how organizations successfully adapt to an increasingly digital environment.

Acknowledgement

This publication was supported by Universiti Teknikal Malaysia Melaka (UTeM) under the Journal Publication Fee Initiative 2025. The authors would also like to acknowledge the support from the Faculty of Technology Management and Technopreneurship.

References

[1] Aggarwal, R. (2024). Evaluating Disaster Recovery Techniques and Business Continuity Models in Cloud Computing. *INTERNATIONAL JOURNAL of ADVANCED RESEARCH in CLOUD COMPUTING (IJARCC)*, *5*(2), 1–5. https://ijarcc.com/index.php/home/article/view/IJARCC.05.02.001.

[2] Akib, H., Furkan, N., Sumarno, S., Budidarma, A., Salam, R., & Hadi, S. (2022). Business Resilience in the Digital Transformation Era. *PINISI Discretion Review*, *6*(1), 95. https://doi.org/10.26858/pdr.v6i1.37708.

[3] Alsaidi, D. H., Shehab, E. (2022). The role of digital technologies in business continuity and resilience: A systematic literature review: Technological Forecasting and Social Change, 178, 121570. https://doi.org/10.1016/j.techfore.2022.121570.

[4] Alshamsi, A. (2024). Integrating and Transforming Business Continuity Management into the Digitalisation. *International Journal of Science and Research (IJSR)*, *13*(2), 1198–1200. https://doi.org/10.21275/SR24212150117.

[5] Awad, J., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*, *13*(1). https://doi.org/10.1186/s13731-024-00405-4.

[6] Banihashemi, S., Hosseini, M. R., Golizadeh, H., & Sankaran, S. (2017). Critical success factors (CSFs) for the integration of sustainability into construction project management practices in developing countries. *International Journal of Project Management*, *35*(6), 1103–1119. https://doi.org/10.1016/j.ijproman.2017.01.014.

[7] Basa, R. (2024). Cloud Disaster Recovery: Best Practices for Business Continuity in the Cloud. *IJFMR240528745*, *6*(5). https://www.ijfmr.com/papers/2024/5/28745.pdf. https://doi.org/10.36948/ijfmr.2024.v06i05.28745.

[8] Bhole, A. (2023). *Cloud Computing for Disaster Recovery and Business Continuity - IJIRCT*. Ijirct.org. https://www.ijirct.org/viewPaper.php?paperId=2501013.

[9] Breidbach, C. F., Joshi, A. M., Twigg, A., & Dickens, G. (2024). Orchestrating Digital Resilience: A Clinical IS Study of an Everything-as-a-Service Technology Strategy. *European Journal of Information Systems*, 1–18. https://doi.org/10.1080/0960085X.2024.2435975.

[10] Browder, R. E., Dwyer, S. M., & Koch, H. (2023). Upgrading adaptation: How digital transformation promotes organizational resilience. *Strategic Entrepreneurship Journal*, *18*(1). https://doi.org/10.1002/sej.1483.

[11] Cardoso, A., Figueiredo, J., Oliveira, I., & Pocinho, M. (2025). From Crisis to Opportunity: Digital Transformation, Digital Business Models, and Organizational Resilience in the Post-Pandemic Era. *Administrative Sciences*, *15*(6), 193. https://doi.org/10.3390/admsci15060193.

[12] Chakravorti, B. (2023). Digital transformation as a resilience driver in turbulent times. *Harvard Business Review*. https://hbr.org.

[13] Chiarini, A., & Vagnoni, E. (2020). Strategy innovation through digital transformation for business continuity in healthcare. *TQM Journal*, 32(5), 951–966.

[14] Ciampi, F., Faraoni, M., Ballerini, J., & Meli, F. (2022). The co-evolutionary relationship between digitalization and organizational agility: Ongoing debates, theoretical developments, and future research perspectives. *Technological Forecasting and Social Change*, *176*, 121383. https://doi.org/10.1016/j.techfore.2021.121383.

[15] Coad, A., & Storey, D. J. (2021). Taking the entrepreneur out of entrepreneurship. *International Journal of Management Reviews*, *23*(4). https://doi.org/10.1111/ijmr.12249.

[16] Deloitte. (2021). *The digital transformation imperative: Lessons from COVID-19*. https://www2.deloitte.com

[17] Elgazzar, Y., El-Shahawy, R., & Senousy, Y. (2021). The Role of Digital Transformation in Enhancing Business Resilience with the Pandemic of COVID-19. *Digital Transformation Technology*, 323–333. https://doi.org/10.1007/978-981-16-2275-5_20.

[18] Ellen, B. P., Mackey, J. D., McAllister, C. P., & Mercer, I. S. (2022). Are small measures big problems? A meta-analytic investigation of brief measures of the Big Five. *Journal of Business Research*, *151*, 579–592. https://doi.org/10.1016/j.jbusres.2022.07.027.

[19] Ellström, D., Holtstrom, J., Berg, E., & Johansson, C. (2021). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*, *15*(2), 272–286. Emerald. https://doi.org/10.1108/JSMA-04-2021-0089.

[20] Felder, R. M., & Prince, M. J. (2025). *Inductive Teaching and Learning Methods: Definitions, Comparisons, and Research Bases*. Per-Central.org. https://www.per-central.org/items/detail.cfm?ID=3593&utm_source=chatgpt.com.

[21] Gao, C., & Yu, J. (2023). SecureRC: A system for privacy-preserving relation classification using secure multi-party computation. *Computers & Security*, *128*, 103142. https://doi.org/10.1016/j.cose.2023.103142.

[22] Gartner. (2022). *Leadership vision for business continuity and risk management*. https://www.gartner.com

[23] George, G., Merrill, R. K., & Schillebeeckx, S. J. D. (2020). Digital transformation, sustainability and purpose in the 2030 Agenda. *Journal of Management Studies*, 57(3), 547–552. https://doi.org/10.1016/j.jwb.2022.101326.

[24] He, Z., Huang, H., Choi, H., & Bilgihan, A. (2022). Building organizational resilience with digital transformation. *Journal of Service Management*, *34*(1), 147–171. https://doi.org/10.1108/JOSM-06-2021-0216.

[25] Hokmabadi, H., Rezvani, S. M. H. S., & de Matos, C. A. (2024). Business Resilience for Small and Medium Enterprises and Startups by Digital Transformation and the Role of Marketing Capabilities—A Systematic Review. *Systems*, *12*(6), 220. https://www.mdpi.com/2079-8954/12/6/220. https://doi.org/10.3390/systems12060220.

[26] Huemann, M., & Silvius, G. (2017). Projects to create the future: Managing projects meets sustainable development. *International Journal of Project Management*, *35*(6), 1066–1070. https://doi.org/10.1016/j.ijproman.2017.04.014.

[27] Jabr, F. (2023). John A. Long - Publications List. *Publicationslist.org*, *14*(6).

[28] Johri, A., & Olds, B. M. (2011). Situated Engineering Learning: Bridging Engineering Education Research and the Learning Sciences. *Journal of Engineering Education*, *100*(1), 151–185. https://doi.org/10.1002/j.2168-9830.2011.tb00007.x.

[29] Lezzi, M., Corallo, A., Lazoi, M., & Nimis, A. (2025). Measuring cyber resilience in industrial IoT: a systematic literature review. *Management Review Quarterly*. https://doi.org/10.1007/s11301-025-00495-8.

[30] Li, W., Yun, K., & Li, F. (2024). The Dynamic Driving Path of Organizational Resilience to Digital Transformation—An Empirical Study Based on TJ-QCA. *Journal of the Knowledge Economy*. https://doi.org/10.1007/s13132-024-02361-6.

[31] Liu, Y., Guo, M., Han, Z., Gavurova Beata, Bresciani, S., & Wang, T. (2023). Effects of digital orientation on organizational resilience: a dynamic capabilities perspective. *Journal of Manufacturing Technology Management*.

[32] Motro, D., Perkins, B. G., & Ellis. (2024). Responses to observing others caught cheating: The role of schadenfreude. *Journal of Management & Organization*, 1–22. https://doi.org/10.1017/jmo.2024.45.

[33] Nasiri, M., Shafiee, S., & Mazdeh, M. M. (2021). Using AI to improve business continuity in supply chain networks. *Journal of Business Research*, 133, 20–32.

[34] Őri, D., Ildikó Szabó, Kő, A., & Tibor Kovács. (2024). Digitalizing in crisis: the role of organizational resilience in SMEs' digitalization. *Journal of Enterprise Information Management*. https://doi.org/10.1108/JEIM-03-2023-0141.

[35] Petropoulou, A., Angelaki, E., Rompogiannakis, I., Passas, I., Garefalakis, A., & Thanasas, G. (2024). Digital Transformation in SMEs: Pre- and Post-COVID-19 Era: A Comparative Bibliometric Analysis. *Sustainability*, *16*(23), 10536. https://doi.org/10.3390/su162310536.

[36] Reddy, S., & Sampath, P. (2024). Reimagining business continuity in the hybrid work era. *MIT Sloan Management Review*, 65(1), 44–51.

[37] Rivera, M., Qiu, L., Kumar, S., & Petrucci, T. (2021). Are traditional performance reviews outdated? An empirical analysis on continuous, real-time feedback in the workplace. *Information Systems Research*, *32*(2), 517–540. https://doi.org/10.1287/isre.2020.0979.

[38] Rupeika-Apoga, R., Petrovska, K., & Bule, L. (2022). The Effect of Digital Orientation and Digital Capability on Digital Transformation of SMEs during the COVID-19 Pandemic. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*(2), 669–685. https://doi.org/10.3390/jtaer17020035.

[39] Russpatrick, S., Sæbø, J., Monteiro, E., Nicholson, B., & Sanner, T. (2021). *Digital Resilience to Covid-19: A Model for National Digital Health Systems to Bounce Forward From the Shock of a Global Pandemic*. ArXiv.org. https://arxiv.org/abs/2108.09720.

[40] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15). https://doi.org/10.3390/s23156666.

[41] Sagala, G. H., & Őri, D. (2024). Exploring digital transformation strategy to achieve SMEs resilience and antifragility: a systematic literature review. *Journal of Small Business & Entrepreneurship*, *37*(3), 1–30. https://doi.org/10.1080/08276331.2024.2392080.

[42] Steen, R., Haug, O. J., & Patriarca, R. (2023). Business continuity and resilience management: A conceptual framework. *Journal of Contingencies and Crisis Management*, *32*(1). https://doi.org/10.1111/1468-5973.12501.

[43] Tarigan, M. K., Simatupang, T. M., & Bangun, Y. R. (2025). Building resilience through digital transformation: a systematic literature review and comprehensive framework for large enterprises. *International Journal of Business Innovation and Research*, *36*(5), 1–28. https://doi.org/10.1504/IJBIR.2025.145665.

[44] Vial, G. (2019). Understanding Digital transformation: a Review and a Research Agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003.

[45] Walther, J., Kellam, N., Sochacka, N., & Radcliffe, D. (2011). Engineering Competence? An Interpretive Investigation of Engineering Students' Professional Formation. *Journal of Engineering Education*, *100*(4), 703–740. https://doi.org/10.1002/j.2168-9830.2011.tb00033.x.

[46] Warner, K. S. R., & Wäger, M. (2019). Building Dynamic Capabilities for Digital transformation: an Ongoing Process of Strategic Renewal. *Long Range Planning*, *52*(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001.

[47] Weeks, J. B., Smith, K. M., & Hulland, J. (2021). Consumer brand curation on social shopping sites. *Journal of Business Research*, *133*, 399–408. https://doi.org/10.1016/j.jbusres.2021.05.010.

[48] World Economic Forum. (2023). *Global Risks Report 2023*. https://www.weforum.org

[49] Yaşar, Şe., Baker, D., Robinson-Kurpius, S., Krause, S., & Roberts, C. (2006). Development of a Survey to Assess K-12 Teachers' Perceptions of Engineers and Familiarity with Teaching Design, Engineering, and Technology. *Journal of Engineering Education*, *95*(3), 205–216. https://doi.org/10.1002/j.2168-9830.2006.tb00893.x.

[50] Yu, L., Pan, X., Cao, X., Hu, P., & Bao, X. (2011). Oxygen reduction reaction mechanism on nitrogen-doped graphene: A density functional theory study. *Journal of Catalysis*, *282*(1), 183–190. https://doi.org/10.1016/j.jcat.2011.06.015.

[51] Zhang, C., Khan, I., Dagar, V., Saeed, A., & Zafar, M. W. (2022). Environmental Impact of Information and Communication technology: Unveiling the Role of Education in Developing Countries. *Technological Forecasting and Social Change*, *178*, 121570. https://doi.org/10.1016/j.techfore.2022.121570.

[52] Zhang, C., Zheng, W., Hong, J., & Kafouros, M. (2021). The role of government policies in explaining the internationalization of Chinese firms. *Journal of Business Research*, *141*. https://doi.org/10.1016/j.jbusres.2021.11.056.

[53] Zhang, J., Li, H., & Zhao, H. (2025). The Impact of Digital Transformation on Organizational Resilience: The Role of Innovation Capability and Agile Response. *Systems*, *13*(2), 75–75. https://doi.org/10.3390/systems13020075.

[54] Zhang, L., Cao, T., & Wang, Y. (2018). The mediation role of leadership styles in integrated project collaboration: An emotional intelligence perspective. *International Journal of Project Management*, *36*(2), 317–330. https://doi.org/10.1016/j.ijproman.2017.08.014.

[55] Zhou, W., Chen, Y., & Yang, C. (2021). Artificial intelligence-enabled decision-making for digital resilience. *Computers & Industrial Engineering*, 154, 107124.