



ARTIFICIAL INTELLIGENCE-ENABLED BUSINESS CONTINUITY MANAGEMENT: AI GOVERNANCE, EMPLOYEE ENGAGEMENT, AND SUSTAINABLE ORGANIZATIONAL PERFORMANCE

Mr. A. Mohammed Asif¹, Dr. L. Rathakrishnan²

¹Ph.D. Part-Time Research Scholar, Department of Rural Industries and Management,
Gandhigram Rural Institute (DTBU), Gandhigram, TN, India.

²Research Guide & Supervisor, Senior Professor, Department of Rural Industries and Management,
Gandhigram Rural Institute (DTBU), Gandhigram, TN, India.

Article DOI: <https://doi.org/10.36713/epra28994>

DOI No: 10.36713/epra28994

ABSTRACT

Business Continuity Management (BCM) has long been concerned with keeping critical activities running when unexpected events interrupt normal operations. Traditionally, organizations have relied on business impact analysis, continuity strategies, documented response procedures, and recovery plans. These practices remain essential, but the disruption environment has changed. Cyber incidents, technology failures, supply-chain interruptions, extreme weather, geopolitical uncertainty, and workforce shortages can develop quickly and interact in ways that are difficult to anticipate through periodic reviews alone. Organizations increasingly need BCM arrangements that can identify warning signs early and support decisions before a disruption becomes a major operational problem.

This article develops an integrated framework that connects AI-enabled BCM capability with employee engagement, human-AI collaboration, organizational resilience, and sustainable organizational performance. AI governance is treated as an important condition that can influence whether these technological capabilities produce useful and trustworthy outcomes. The framework draws mainly on Dynamic Capability Theory and Socio-Technical Systems Theory. Recent research on AI and organizational resilience provides encouraging evidence, while emerging work on human-AI collaboration highlights the importance of employee acceptance, skills, and judgment. The article translates these ideas into research objectives, questions, hypotheses, measurement dimensions, and a PLS-SEM research design that can be tested in a subsequent empirical study.

KEYWORDS: Artificial Intelligence; Business Continuity Management; AI Governance; Employee Engagement; Human-AI Collaboration; Organizational Resilience; Sustainable Organizational Performance; Predictive Resilience; Dynamic Capabilities.

1. INTRODUCTION

Organizations now operate through tightly connected technologies, people, suppliers, and digital services. As a result, a disruption in one area can quickly affect several others. A cloud outage, for example, may interrupt customer service, payment processing, employee access, and supplier coordination at the same time. This interconnected environment makes continuity management more demanding than simply maintaining a recovery plan. BCM needs to help organizations recognize changing conditions, understand dependencies, and act while there is still time to reduce the impact.

For this reason, BCM cannot rely only on static plans that are activated once an incident has already occurred. Periodic reviews and exercises are useful, but they may not capture fast-moving or unfamiliar threats. A more forward-looking approach combines established BCM practices with continuous monitoring, data analysis, and informed human judgment.

ISO 22301:2019 presents BCM as a management system rather than as a single document. It covers planning, implementation, operation, monitoring, review, maintenance, and

continual improvement. The purpose is to help organizations protect against disruptive events, reduce the likelihood and consequences of disruption, and recover in a structured way (ISO, 2019). In 2026, ISO is also developing a third edition of the standard; because that edition remains a committee draft, it should not be treated as the current published requirement.

Artificial Intelligence offers a practical way to extend these established BCM activities. Machine learning, natural language processing, anomaly detection, and predictive analytics can examine large volumes of information and highlight patterns that may otherwise be missed. Within BCM, these capabilities can support risk sensing, business impact analysis, scenario development, crisis decision-making, and recovery planning. Recent research has also begun to examine AI directly within BCM and reports potential benefits for early disruption detection and recovery in production settings.

The same technology, however, introduces risks that BCM teams cannot ignore. Poor data, model drift, opaque recommendations, privacy problems, cyberattacks against AI systems, and excessive reliance on automation can create new vulnerabilities. ISO/IEC 42001:2023 provides a management-



system approach for governing AI-related risks and opportunities, with attention to responsible use, transparency, traceability, and reliability (ISO, 2023). In continuity management, these controls matter because an AI recommendation may influence decisions made under severe time pressure.

People remain at the centre of continuity decisions. During a disruption, employees interpret information, question assumptions, communicate with stakeholders, and make judgments when the available evidence is incomplete. AI can support this work, but it cannot remove the need for accountability and contextual knowledge. Employees must be able to understand AI outputs, recognize when an answer is questionable, and intervene when necessary.

Based on this reasoning, the article brings together five elements: AI-enabled BCM capability, employee engagement and human–AI collaboration, organizational resilience, AI governance, and sustainable organizational performance. The central argument is that AI is most valuable when it becomes part of a well-governed organizational capability rather than being introduced as a stand-alone technology project.

2. EVOLUTION OF BUSINESS CONTINUITY MANAGEMENT

The early development of BCM was closely associated with contingency planning and disaster recovery. Organizations focused on protecting critical processes, maintaining backups,

arranging alternative facilities, and restoring essential services after an incident. Over time, BCM became broader. Business impact analysis, supplier continuity, crisis management, testing, exercising, risk integration, and continual improvement became part of a more systematic approach.

ISO 22301:2019 reflects this broader management-system view. Continuity is treated as an ongoing organizational discipline involving planning, implementation, operation, monitoring, review, maintenance, and improvement. This is important because resilience cannot be created by a plan alone; it depends on capabilities that remain useful as the business and threat environment change.

Even well-developed BCM programmes can be heavily dependent on periodic assessments and manual interpretation. Risk registers may be reviewed at fixed intervals, BIA information may be refreshed annually, and exercises may follow a predetermined schedule. Such activities provide a necessary foundation, but they may leave a gap between the speed of change in the external environment and the speed at which the organization updates its understanding of risk.

Predictive resilience shifts the emphasis. Instead of asking only how quickly an organization can recover after a disruption, it asks whether the organization can recognize developing problems, prepare while options are still available, and adapt as conditions change. AI can contribute to this shift by strengthening the sensing and analytical capabilities already present within the BCMS.

Table 1. Transition from Traditional BCM to AI-Enabled Predictive Resilience

Dimension	Traditional / Reactive BCM	AI-Enabled / Predictive BCM
Risk identification	Periodic assessments and expert review	Continuous sensing, pattern recognition and predictive risk analytics
Business Impact Analysis	Manual or periodic data collection	AI-assisted impact modelling and dynamic dependency analysis
Monitoring	Rule-based alerts and dashboards	Anomaly detection, multi-source signal fusion and predictive alerts
Scenario planning	Predefined scenarios and workshops	AI-supported scenario generation, simulation and stress testing
Crisis decision-making	Human-led analysis under time pressure	AI-assisted decision support with human validation
Recovery	Plan-based restoration	Risk-informed, dynamically optimized recovery sequencing
Learning	Post-incident reviews	Continuous learning from incidents, near misses and operational data

3. ARTIFICIAL INTELLIGENCE IN BUSINESS CONTINUITY MANAGEMENT

3.1 AI-Enabled Risk Prediction

AI-enabled risk prediction uses machine learning, statistical methods, natural language processing, and related techniques to identify patterns that may signal disruption. Relevant information can come from incident records, service metrics, cyber telemetry, supplier data, weather information, operational reports, and other internal or external sources. The important point for BCM is not prediction for its own sake. The value comes when an early signal leads to a practical continuity action.

3.2 Intelligent Monitoring and Anomaly Detection

Continuous monitoring allows an organization to notice changes from expected operating conditions. AI-based anomaly detection can be applied to system availability, transaction volumes, network behaviour, supply indicators, workforce availability, and customer demand. When these signals are connected to clear BCM thresholds and escalation procedures, the organization has a better chance of moving from detection to action before the disruption spreads.



3.3 AI-Supported Business Impact Analysis

Business Impact Analysis remains one of the foundations of BCM because it identifies what matters most, what dependencies exist, and what the consequences of interruption may be. AI can help analyse relationships among processes, applications, suppliers, locations, data, roles, and customers. It can also assist with extracting information from policies, process documents, incident reports, and previous BIA records. Business owners must still validate the results because criticality is not purely a statistical question; regulatory obligations, customer commitments, strategic priorities, and ethical considerations also matter.

3.4 Scenario Intelligence and Stress Testing

AI can also broaden the way organizations think about scenarios. Instead of relying only on a fixed list of exercises, AI-supported analysis can combine historical events with hypothetical conditions and explore compound disruptions. Examples include a cyberattack occurring alongside a supplier outage, extreme weather combined with staff shortages, or a technology failure during an unexpected surge in customer demand. Such analysis can complement, rather than replace, traditional tabletop exercises and stress testing.

3.5 AI-Assisted Crisis Decision-Making

During a crisis, decision-makers often have to bring together information from many sources in a very short time. AI can help summarize situation reports, identify dependencies, compare response options, and highlight information gaps. Its role should remain decision support. For high-impact continuity decisions, organizations need clear human decision rights, escalation arrangements, and the ability to override an AI recommendation when professional judgment indicates that it is unsafe or inappropriate.

3.6 Predictive Recovery and Continuous Learning

Recovery is another area where AI may add value. Models can help compare restoration sequences, identify resource constraints, and estimate the likely business consequences of different recovery choices. After an incident, AI can examine service records, communications, incident logs, and lessons learned to identify recurring patterns. Over time, this creates a feedback loop in which experience from incidents and exercises informs the next cycle of continuity planning.

4. AI GOVERNANCE AS A CORE BCM CAPABILITY

AI governance refers to the arrangements used to decide who is responsible for AI, how risks are assessed, what controls are required, and how important decisions are monitored. In BCM, governance deserves particular attention because AI may influence recovery priorities and crisis responses when the consequences of an error are high.

ISO/IEC 42001:2023 provides a management-system framework for organizations that develop or use AI. It addresses the management of AI-related risks and opportunities and supports responsible practices such as transparency and traceability. NIST's AI Risk Management Framework also organizes AI risk management around Govern, Map, Measure,

and Manage, with governance treated as a cross-cutting function. These approaches are useful complements to BCM, particularly where AI, enterprise risk, cybersecurity, privacy, and operational governance overlap.

For this study, AI governance is represented by accountability, transparency, explainability, data governance, privacy and security, human oversight, and model monitoring. These dimensions are research constructs rather than a claim that any single standard uses exactly the same measurement structure. Their purpose is to capture the organizational conditions that make AI-supported continuity decisions more dependable.

5. EMPLOYEE ENGAGEMENT AND HUMAN-AI COLLABORATION

Employee engagement matters to BCM because continuity work is carried out by people. Employees gather information, follow or adapt procedures, communicate with colleagues and customers, and contribute to recovery. Kahn (1990) linked personal engagement to psychological meaningfulness, safety, and availability, while later work such as Saks (2006) examined the organizational conditions and consequences associated with engagement.

Kahn's foundational work conceptualized personal engagement through psychological meaningfulness, safety, and availability (Kahn, 1990). Later engagement research has examined how organizational conditions and job resources shape employee engagement (Saks, 2006).

AI can improve the employee experience when it removes repetitive work, makes useful information easier to access, and gives employees better support when decisions have to be made quickly. The opposite can also happen. Monitoring concerns, fear of job loss, reduced autonomy, poor training, or unexplained AI decisions may create resistance and disengagement. The effect of AI on employees is therefore unlikely to be uniformly positive or negative.

Human-AI collaboration describes a working arrangement in which people and AI systems contribute different strengths. AI can process information and identify patterns at scale, while employees provide context, experience, ethical judgment, creativity, and accountability. Recent research on human-AI collaboration and team resilience suggests that perceived usefulness, acceptance, and employee capability are important in determining whether this relationship works well.

Within BCM, employee engagement is more than an HR measure. Engaged employees are more likely to participate in exercises, learn new tools, report weak signals, question questionable recommendations, and contribute lessons after an incident. Human-AI collaboration can therefore act as the link between technical capability and practical resilience.

6. ORGANIZATIONAL RESILIENCE

Organizational resilience is the capacity to anticipate disruption, prepare for it, respond when it occurs, recover important functions, and adapt after the event. The concept goes beyond restoring the status quo. A resilient organization also learns from disruption and changes its practices when the



environment demands it.

Recent research provides growing support for a connection between AI and resilience. Ma et al. (2026), for example, found that different forms of AI use can contribute to organizational resilience through AI-enabled sensing, operationalization, and reconstruction capabilities. Other recent studies report positive relationships between AI adoption and resilience in different organizational settings. Research focused specifically on BCM has likewise begun to examine how AI can improve early detection and recovery.

For the present study, resilience is considered through six related capabilities: anticipation, preparedness, response, adaptation, recovery, and learning. These dimensions connect formal BCM activities with the broader ability of an organization to cope with uncertainty. AI may strengthen each capability, but the outcome is likely to depend on governance, organizational readiness, employee skills, and the quality of the data and processes supporting the technology.

This means that AI should not be treated as a universal solution. The same technology may produce different results in organizations with different levels of digital maturity, governance discipline, employee capability, and data quality. Resilience is ultimately an organizational outcome, not simply a technical feature.

7. SUSTAINABLE ORGANIZATIONAL PERFORMANCE

Sustainable organizational performance refers to the ability to maintain useful organizational outcomes over time while balancing operational, financial, customer, employee, and longer-term strategic needs. In a BCM context, this means that continuity arrangements should do more than reduce immediate losses. They should also help the organization maintain reliable services, preserve stakeholder confidence, support employees, and learn from disruption.

Recent studies suggest that AI can contribute to sustainable performance when it becomes embedded in broader organizational capabilities. The important mechanism is not the technology by itself but what the organization is able to do with it: sense change, learn, redesign processes, and reconfigure resources. This perspective fits well with the dynamic capability logic used in the present study.

The framework therefore treats organizational resilience as a key pathway between AI-enabled BCM and sustainable performance. An organization that can anticipate problems, respond effectively, adapt its processes, recover critical services, and learn from experience is better placed to protect both short-term operations and longer-term performance.

8. REVIEW OF LITERATURE

8.1 AI and Organizational Resilience

Recent studies increasingly view AI as an organizational capability rather than simply an IT application. Ma et al. (2026) examined purpose-specific AI use and organizational resilience using PLS-SEM and fuzzy-set qualitative comparative analysis. Their findings indicate that work-oriented and social-oriented AI

use can strengthen resilience through AI-enabled sensing, operationalization, and reconstruction. The study also points to the importance of a data-driven culture, suggesting that organizational context influences how much value AI creates.

Research on SMEs also points in a similar direction. Peng, Li, and Hu (2026) reported a positive association between AI adoption and organizational resilience, while highlighting the role of innovation capabilities and environmental unpredictability. This suggests that resilience is shaped by a combination of technology and organizational conditions rather than by technology adoption alone.

Żywiołek (2026) is particularly relevant to this study because the research directly examines AI in business continuity management and the resilience of production systems. The study presents AI as part of a broader continuity and security architecture and reports potential benefits in early disruption detection, limiting cascading effects, and improving recovery dynamics.

8.2 Human-AI Collaboration and Employee Outcomes

Liu et al. (2026) examined human-AI collaboration in relation to team resilience and identified perceived usefulness and AI teammate acceptance as important mechanisms, with team skill level affecting the strength of the relationship. Zhao et al. (2026) similarly examined human-AI collaboration and employee thriving, pointing to mechanisms such as cognitive reframing and informal learning. Together, these studies support the idea that the human side of AI adoption deserves a central place in resilience research.

Research on AI-enabled HR analytics also shows that technology can create both resources and demands. AI may improve access to information and support better decisions, but it can also increase digital pressure or concerns about monitoring and autonomy. This mixed picture reinforces the need to consider employee capability, trust, participation, and governance when examining AI-enabled BCM.

8.3 AI Governance and Sustainability

AI governance can contribute to sustainability by turning AI use into repeatable and accountable organizational practice. Governance arrangements help clarify responsibilities, establish controls, and create feedback mechanisms through which the organization can learn from AI-related successes and failures. Recent work on AI governance and sustainability emphasizes the importance of organizational sensemaking, ethical framing, participation, governance routines, and feedback. These ideas are consistent with the view that responsible AI is not achieved through a policy document alone; it has to become part of everyday decision-making and organizational learning.

ISO/IEC 42001 offers a practical management-system foundation for this governance perspective. In the present framework, AI governance is treated as a moderator. The expectation is that AI-enabled BCM will contribute more strongly to resilience when the technology is supported by clear accountability, trustworthy data, appropriate oversight, and ongoing monitoring.



9. RESEARCH GAP

The literature points to several areas that still need closer examination. First, AI and BCM have often developed as separate research streams, and relatively few studies bring them together as an integrated organizational capability. Second, research linking AI with resilience frequently focuses on technology adoption or dynamic capabilities without fully incorporating the formal processes of BCM. Third, human factors such as employee engagement, AI acceptance, trust, and human oversight have received less attention than the technology itself. Finally, AI governance and sustainable organizational performance are rarely examined together within the same BCM model.

This study addresses that intersection. It does not assume that adopting AI automatically creates resilience. Instead, it argues that AI-enabled BCM becomes valuable when employees can work effectively with the technology, when governance mechanisms make its use trustworthy, and when the organization is capable of converting information into anticipation, response, adaptation, recovery, and learning.

10. RESEARCH OBJECTIVES

- To examine the role of Artificial Intelligence in Business Continuity Management.
- To identify the major dimensions of AI-enabled BCM capability.
- To examine the influence of AI-enabled BCM capability on employee engagement and human-AI collaboration.
- To examine the influence of AI-enabled BCM capability on organizational resilience.
- To investigate the role of human-AI collaboration in strengthening organizational resilience.
- To examine the moderating role of AI governance in the relationship between AI-enabled BCM capability and organizational resilience.
- To examine the influence of organizational resilience on sustainable organizational performance.
- To develop an integrated AI-enabled BCM framework suitable for empirical validation using PLS-SEM.

11. RESEARCH QUESTIONS

- How does AI-enabled BCM capability influence organizational resilience?
- How does AI-enabled BCM capability influence employee engagement and human-AI collaboration?
- Does human-AI collaboration mediate the relationship between AI-enabled BCM capability and organizational resilience?

- Does AI governance strengthen the relationship between AI-enabled BCM capability and organizational resilience?
- Does organizational resilience mediate the relationship between AI-enabled BCM capability and sustainable organizational performance?

12. THEORETICAL FOUNDATIONS

12.1 Dynamic Capability Theory

Dynamic Capability Theory is useful here because organizations operating in uncertain environments need to sense changes, seize opportunities or respond to threats, and reconfigure resources. AI-enabled BCM can support each of these activities. It can improve the organization's ability to notice weak signals, evaluate possible consequences, and adjust continuity resources before or during a disruption.

12.2 Socio-Technical Systems Theory

Socio-Technical Systems Theory adds the human and organizational side of the explanation. AI models, data, systems, employees, processes, leadership, and governance do not operate independently. Their interaction shapes the quality of the final outcome. This makes the theory particularly suitable for studying human-AI collaboration and employee engagement within BCM.

12.3 Complementary Governance Perspective

AI governance provides a complementary control perspective. The framework assumes that the benefits of AI depend on how responsibly it is introduced and used. Accountability, transparency, data governance, security, human oversight, and monitoring can determine whether an AI capability becomes a dependable organizational resource or a new source of operational risk.

13. CONCEPTUAL FRAMEWORK

AI-Enabled BCM Capability → Human-AI Collaboration → Organizational Resilience → Sustainable Organizational Performance

AI Governance moderates the relationship between AI-Enabled BCM Capability and Organizational Resilience.

The framework follows a sequential logic. AI-enabled BCM capability gives the organization better ways to sense, analyze, predict, and respond to disruption. When employees find the technology useful and trustworthy, they are more likely to engage with it and work alongside it. Effective human-AI collaboration can then strengthen resilience by improving anticipation, preparedness, response, adaptation, recovery, and learning. Stronger resilience should, in turn, support more sustainable organizational performance. AI governance is expected to strengthen the technology-to-resilience link by creating the conditions for responsible and reliable use.



Table 2. Constructs and Proposed Dimensions

Construct	Role	Proposed dimensions
AI-enabled BCM capability	Independent variable	Risk prediction; intelligent monitoring; AI-supported BIA; scenario intelligence; AI decision support; predictive recovery
Human–AI collaboration	Mediator	AI trust; perceived usefulness; AI competence; human oversight; joint decision-making; employee participation
Employee engagement	Complementary human factor	Vigour; dedication; absorption; participation in continuity activities; willingness to learn
Organizational resilience	Mediator / outcome	Anticipation; preparedness; response; adaptation; recovery; learning
AI governance	Moderator	Accountability; transparency; explainability; data governance; security/privacy; human oversight; monitoring
Sustainable organizational performance	Dependent variable	Operational; financial; customer; employee; strategic/long-term performance

14. HYPOTHESES DEVELOPMENT

H1 – AI-enabled BCM capability is positively associated with human–AI collaboration.

H2 – AI-enabled BCM capability is positively associated with organizational resilience.

H3 – AI-enabled BCM capability is positively associated with employee engagement.

H4 – Human–AI collaboration is positively associated with organizational resilience.

H5 – Employee engagement is positively associated with organizational resilience.

H6 – Organizational resilience is positively associated with sustainable organizational performance.

H7 – AI-enabled BCM capability is positively associated with sustainable organizational performance.

H8 – Human–AI collaboration mediates the relationship between AI-enabled BCM capability and organizational resilience.

H9 – Organizational resilience mediates the relationship between AI-enabled BCM capability and sustainable organizational performance.

H10 – Human–AI collaboration and organizational resilience sequentially mediate the relationship between AI-enabled BCM capability and sustainable organizational performance.

H11 – AI governance positively moderates the relationship between AI-enabled BCM capability and organizational resilience, with a stronger relationship expected when AI governance is stronger.

15. RESEARCH METHODOLOGY

15.1 Research Design

The empirical phase is designed as a quantitative, cross-sectional survey. It will focus on organizations in which BCM, risk management, IT disaster recovery, cyber security, operations, or AI-supported decision-making are relevant. A

survey approach is appropriate for testing relationships among the proposed latent constructs and for examining indirect and interaction effects.

15.2 Population and Respondents

The target respondents will be professionals who have practical exposure to BCM, IT disaster recovery, enterprise risk, cybersecurity, information technology, operations, AI or data analytics, crisis management, or related activities. Possible respondents include BCM and ITDR managers, risk and cybersecurity professionals, technology and operations managers, and other business leaders familiar with organizational continuity arrangements.

15.3 Sample Size

A target of around 400–500 usable responses is recommended for the empirical phase. The final sample requirement should also be checked through an a priori power analysis based on the number of predictors and the complexity of the model. The larger target is intended to provide enough information for testing direct paths as well as mediation, moderation, and selected subgroup differences.

15.4 Sampling Technique

Purposive sampling can be used to reach respondents who have relevant professional knowledge. Where appropriate, respondents may also be reached through professional networks and referrals. Screening questions should be included so that the final sample is not dominated by participants who have no meaningful exposure to BCM or AI-enabled organizational processes.

15.5 Questionnaire Design

The questionnaire will use a five-point Likert scale, from 1 = Strongly Disagree to 5 = Strongly Agree. Wherever possible, measurement items should be adapted from established scales and then contextualized for BCM. Before the main survey, a pilot study should be conducted to check clarity, reliability, completion time, and whether respondents interpret the items as intended.



Table 3. Proposed Measurement Blueprint

Construct	Indicative dimensions	Indicative item themes	Expected role
AI-enabled BCM capability	Prediction, monitoring, BIA, scenario analysis, decision support, recovery	Our organization uses AI to identify emerging continuity risks; AI supports impact analysis; AI assists continuity decisions	Independent
Human–AI collaboration	Trust, usefulness, competence, oversight, joint decisions	Employees understand AI recommendations; humans validate important AI outputs; AI supports rather than replaces critical judgment	Mediator
Employee engagement	Vigour, dedication, participation, learning	Employees actively participate in continuity activities; employees are willing to learn AI-enabled BCM processes	Complementary mediator/predictor
Organizational resilience	Anticipation, preparedness, response, adaptation, recovery, learning	The organization detects disruption early; adapts processes quickly; learns from incidents	Mediator
AI governance	Accountability, transparency, data, security, oversight, monitoring	AI responsibilities are defined; important AI decisions are explainable; AI systems are monitored	Moderator
Sustainable organizational performance	Operational, financial, customer, employee, strategic	Continuity capabilities support stable operations, customer confidence, employee effectiveness and long-term performance	Dependent

16. PROPOSED DATA ANALYSIS

PLS-SEM is recommended because the study is primarily prediction-oriented and includes several latent constructs together with mediation and moderation paths. The analysis can be organized into two broad stages: first, establishing that the measurement model is reliable and valid; and second, assessing the relationships proposed in the structural model.

16.1 Measurement Model

- Indicator reliability should be assessed using standardized outer loadings, alongside the substantive relevance of each item.
- Internal consistency should be examined using Cronbach's alpha and composite reliability.
- Convergent validity should be assessed through Average Variance Extracted (AVE).
- Discriminant validity should be examined using HTMT and supporting indicator-level evidence.
- Collinearity should be checked using appropriate VIF diagnostics.

16.2 Structural Model

- Estimate path coefficients and their significance using bootstrapping.
- Report R^2 values for the endogenous constructs.
- Examine f^2 to understand the contribution of individual

predictors.

- Assess predictive relevance (Q^2) where appropriate.
- Test indirect effects to evaluate mediation.
- Assess the AI governance interaction using an appropriate PLS moderation procedure.
- Where theoretically justified, compare groups such as organization size, sector, AI maturity, or respondent role.

16.3 Common Method Bias and Data Quality

Because the main constructs are likely to be measured through the same questionnaire, common method bias needs to be considered. The study should use practical procedural safeguards such as anonymous participation, clear and neutral wording, and separation of predictor and outcome sections where possible. Statistical checks can then be used as an additional diagnostic rather than as the sole basis for judging common method bias.

17. PROPOSED AI-ENABLED BCM MATURITY MODEL

The five-level maturity model is intended to provide a simple way of describing how organizations may progress from basic continuity planning to more adaptive, AI-supported resilience. It is a research framework rather than an established industry standard and should be refined through empirical testing.



Level	Maturity state	Characteristics
Level 1	Reactive	Manual plans; incident-driven response; limited analytics; periodic reviews.
Level 2	Digitized	Digital BCM documentation, dashboards, workflow and reporting.
Level 3	AI-Assisted	AI supports risk analysis, BIA, monitoring and decision-making with human review.
Level 4	Predictive	AI predicts emerging disruption, estimates impacts and supports proactive intervention.
Level 5	Adaptive	Continuous sensing, prediction, human-AI collaboration, automated learning and dynamic adaptation.

18. DISCUSSION AND EXPECTED THEORETICAL CONTRIBUTION

The framework makes several theoretical contributions. First, it moves the discussion of BCM beyond the traditional emphasis on plans and recovery toward predictive and adaptive resilience. The distinction matters because organizations increasingly need to identify emerging problems while there is still time to act.

The second contribution is the connection between BCM and Dynamic Capability Theory. AI is treated not merely as an information system but as a capability that can improve organizational sensing and reconfiguration. This helps explain why the value of AI may differ across organizations even when they use similar technologies.

The third contribution is socio-technical. By including human-AI collaboration and employee engagement, the framework recognizes that continuity technology only creates value when people understand it, use it appropriately, and are willing to challenge it when necessary. Employees remain essential for contextual judgment, communication, accountability, and adaptation.

The fourth contribution concerns governance. AI governance is positioned as a boundary condition rather than an additional technology variable. This reflects the possibility that identical AI capabilities can produce very different outcomes depending on transparency, data quality, security, oversight, and organizational accountability.

Fourth, the model positions AI governance as a boundary condition. This is important because the same AI capability may generate different outcomes depending on transparency, data governance, security, oversight, and organizational accountability. The framework therefore avoids technological determinism.

19. MANAGERIAL IMPLICATIONS

- Organizations should integrate AI-enabled risk sensing with existing BCM governance rather than operating AI

experiments as isolated technology projects.

- BCM teams should establish clear human decision rights for AI-assisted crisis decisions, including escalation and override mechanisms.
- AI governance should be aligned with BCM, enterprise risk, cyber security, privacy, and information-security governance.
- Organizations should invest in employee AI literacy and BCM capability so that staff can interpret, challenge, and appropriately use AI outputs.
- AI-enabled BIA should be periodically validated against business-owner knowledge and changes in technology, suppliers, customers, and regulations.
- Continuity exercises should include AI failure scenarios, model errors, data-quality problems, cyber compromise of AI systems, and loss of AI services.
- Organizations should create feedback loops so that incident lessons, near misses, exercise results, and employee observations improve future AI-enabled continuity processes.
- Sustainability should be evaluated not only through financial outcomes but also through operational reliability, customer confidence, employee outcomes, and adaptive capability.

20. AI GOVERNANCE REQUIREMENTS FOR AI-ENABLED BCM

An AI-enabled BCMS needs controls that cover the AI lifecycle as well as the continuity lifecycle. Responsibilities should be clear for model ownership, data ownership, validation, risk acceptance, escalation, and human oversight. Technical controls should address model performance, data quality, access, cybersecurity, drift, and availability.

The level of transparency should match the importance of the decision. A routine recommendation may require basic traceability, whereas an AI recommendation that changes recovery priorities or affects customers may require documented



human approval. Organizations should also maintain fallback procedures for situations in which an AI service is unavailable. If AI becomes a critical dependency, it belongs in the BIA, risk assessment, recovery strategy, and testing programme just like any other critical service.

21. RISKS AND LIMITATIONS OF AI-ENABLED BCM

- Data quality and representativeness can reduce predictive reliability.
- Model drift may make historical relationships less useful as disruption patterns change.
- Black-box recommendations can weaken trust and accountability.
- Cyberattacks may target AI models, training data, interfaces, or supporting infrastructure.
- Overreliance on AI may create automation bias and reduce human challenge.
- AI systems may introduce privacy and regulatory risks when processing sensitive organizational or employee data.
- AI availability can become a continuity dependency requiring its own recovery arrangements.
- Employee resistance or insufficient AI literacy may limit adoption.
- Generative AI may produce inaccurate or fabricated information and therefore requires validation controls.
- Cross-sectional survey research cannot establish causal direction as strongly as longitudinal or experimental designs.

22. FUTURE RESEARCH

Future research should test the framework across industries, organization sizes, and countries. Longitudinal studies would be particularly useful because they could examine whether AI-enabled BCM actually improves resilience over time rather than simply being associated with it at one point. Multi-level studies could also connect individual employee attitudes with team processes and organizational governance. Case studies of real disruptions would provide another valuable way to compare AI-assisted and conventional response practices.

Another important area is the continuity of the AI systems themselves. Future research should examine model failure, data poisoning, adversarial manipulation, loss of AI service availability, governance failures, and the consequences of inaccurate generative-AI outputs. Researchers could also test the five-level maturity model and determine whether higher AI-enabled BCM maturity is associated with measurable improvements in resilience and performance.

23. LIMITATIONS

This article presents a conceptual research framework rather than completed empirical findings. The relationships described here are theoretically grounded and supported by recent literature, but they remain hypotheses until original data are collected and

analysed. A cross-sectional survey would also limit strong causal interpretation. In addition, AI adoption and BCM maturity vary considerably between sectors and organizations, so measurement items may need to be adapted to the context in which the study is conducted.

24. CONCLUSION

BCM is gradually moving from a discipline centered on recovery toward one that also emphasizes anticipation and adaptation. AI can support this shift by helping organizations monitor signals, assess risk, analyse dependencies, explore scenarios, and make better-informed recovery decisions. The technology is promising, but it is not a substitute for sound BCM processes or human judgment.

The framework developed in this article connects AI-enabled BCM capability with employee engagement and human-AI collaboration, organizational resilience, and sustainable organizational performance, while giving AI governance a central moderating role. This combination brings together technical, behavioral, governance, and resilience perspectives that are often studied separately.

The central message is straightforward: the future of BCM is not only about recovering faster after something goes wrong. It is about becoming better at noticing change, preparing early, making informed decisions, adapting under pressure, and learning after the event. AI can help organizations achieve that goal when it is introduced with appropriate governance and when employees are equipped to work with it rather than simply being expected to follow it.

REFERENCES

1. *Academy of Management Proceedings*. (2026). *A study on the impact of human-AI collaboration on team resilience*. <https://doi.org/10.5465/AMPROC.2026.129bp>
2. Floridi, L., Cowls, J., Beltracchi, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). *AI4People – An ethical framework for a good AI society*. *Minds and Machines*, 28, 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
3. ISO. (2019). *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements*. International Organization for Standardization.
4. ISO. (2023). *ISO/IEC 42001:2023 Information technology – Artificial intelligence – Management system*.
5. International Organization for Standardization.
6. Javed, M. (2026). *Harnessing artificial intelligence and employee resilience for enhanced business performance: A resource-based and dynamic capabilities perspective*. *Human Behavior and Emerging Technologies*. <https://doi.org/10.1155/hbe2/1701203>
7. Jobin, A., Ienca, M., & Vayena, E. (2019). *The global landscape of AI ethics guidelines*. *Nature Machine Intelligence*, 1, 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
8. Kahn, W. A. (1990). *Psychological conditions of personal engagement and disengagement at work*.
9. *Academy of Management Journal*, 33(4), 692–724. <https://doi.org/10.2307/256287>
10. Liu, Y., Shi, Y., Bu, W., & Li, J. (2026). *A study on the impact of human-AI collaboration on team resilience*. *Academy of*



Management Proceedings.

<https://doi.org/10.5465/AMPROC.2026.129bp>

11. Ma, L., Qi, Z., Zhang, X., Hao, F., & Chi, M. (2026). *How purpose-specific AI use builds organizational resilience: A dynamic capability perspective*. *Technology in Society*, 86, 103311. <https://doi.org/10.1016/j.techsoc.2026.103311>
12. Peng, P., Li, X., & Hu, H. (2026). *Artificial intelligence adoption and organizational resilience in SMEs: The roles of ambidextrous innovation and environmental unpredictability*. *Humanities and Social Sciences Communications*.
13. Saks, A. M. (2006). *Antecedents and consequences of employee engagement*. *Journal of Managerial Psychology*, 21(7), 600–619. <https://doi.org/10.1108/02683940610690169>
14. Wang, Y., Gao, X., Fu, L., & Chen, Z. (2026). *AI-enabled open innovation: A contingency approach to building organizational resilience*. *Technology in Society*, 88, 103462.
15. Zhang, M., & Dong, W. (2026). *Artificial intelligence assimilation shapes sustainable performance through dynamic capabilities*. *Scientific Reports*, 16, 16619. <https://doi.org/10.1038/s41598-026-46291-6>
16. Zhao, X., Xi, M., Yin, Y., Zhou, Y., & Wang, X. (2026). *Human-AI collaboration enables employee thriving at work: A dual-pathway mechanism based on SDT*. *Academy of Management Proceedings*. <https://doi.org/10.5465/AMPROC.2026.15746>
17. Żywiłtek, J. (2026). *Artificial intelligence in business continuity management and the resilience of production systems to safety disruptions*. *Management Systems in Production Engineering*, 34(2). <https://doi.org/10.2478/mspe-2026-0027>
18. Nguyen, M., Nham, T. P., Alghafes, R., Rahman, O., & Imre, G. (2026). *Human-GenAI-based agent collaboration: How employee perceptions shape knowledge sharing, thriving, and well-being*. *Acta Psychologica*, 263, 106271. <https://doi.org/10.1016/j.actpsy.2026.106271>