systems

MDPI

Article

Building a Strategic System for Resilience in a Risky World

Lisa L. Greenwood [1,*], Dawn Hess [1] and Jennifer Schneider [2]

[1] Department of Civil Engineering Technology, Environmental Management and Safety, College of Engineering Technology, Rochester Institute of Technology, Rochester, NY 14623, USA
[2] Collaboratory for Resiliency & Recovery, Department of Civil Engineering Technology, Environmental Management and Safety, College of Engineering Technology, Rochester Institute of Technology, Rochester, NY 14623, USA
* Correspondence: llgcem@rit.edu

Abstract

The world and its operations are becoming increasingly risky and brittle, with organizations and communities facing escalating threats from both internal and external sources. Risk management and business systems exist to help navigate both acute shocks and chronic stressors, but the decisive factor is how entities plan and respond. This article explores the strategic application of systematic resilience planning across risk types and presents an integrated application for implementation grounded in risk management and business continuity systems standards. The article also explores how these standards can support the identification and treatment of organizational risks and vulnerabilities to provide a clear path to resilience. No risk environment is static. Applied as a dynamic framework that is responsive to evolving risk contexts, a systematic approach offers a powerful path forward in an era of compounding disruption.

Keywords: complex systems; socio-technical systems; emerging social systems; complexity; business continuity; risk management; resilience; sustainability

check for updates

Academic Editor: Giuliano Punzo

Received: 28 July 2025
Revised: 3 September 2025
Accepted: 8 September 2025
Published: 15 September 2025

Citation: Greenwood, L.L.; Hess, D.; Schneider, J. Building a Strategic System for Resilience in a Risky World. *Systems* **2025**, *13*, 805. https://doi.org/10.3390/systems13090805

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Modern systems—including logistics, public health, and information networks—are more interconnected than ever, and thus more vulnerable. At the same time, risk exposure is increasing due to broad disruptive threats, such as those related to global geopolitical volatility, cyber dependencies, workforce or enterprise churn, and climate change. Many organizations now find themselves facing either sudden disruptions or chronic, slow-burning risks that accumulate over time. In both contexts, risk management (RM) alone is insufficient. The capability to maintain operational continuity—before, during, and after a disruption—has become a core requirement for resilience, from survival to success. While traditional risk assessments (RA) are useful, they are often siloed and threat-specific. Today's risks, however, are increasingly interdependent: a natural disaster may cause information technology (IT) outages, for example, which in turn compromise healthcare services or financial operations. These cross-sector linkages increase system brittleness and reduce time for corrective action. Power grid failures, global microchip shortages, and even pandemic responses offer clear evidence that our systems are not just at risk; they are vulnerable and fragile. For each system to gain robustness, the underlying organizational components must also be resilient.

Traditional RA approaches have been based on probabilities, or the likelihood of impacts associated with specific types of hazards and exposures. As we face increasing risk

exposure, such approaches have become inadequate, particularly for more complex systems with high levels of uncertainty and potential for surprises [1]. Integrated Systems for Risk and Continuity Planning (SRCP) offer a structured yet flexible approach to safeguard and advance core operations across any risk type and level of complexity. Rather than focusing on individual hazards in specific disciplines, such frameworks begin with the question, "What must continue, no matter what?" coupled with "what operations and outputs grow our opportunities?" This approach enables planning for service degradation, partial functionality, and layered recovery over time, as well as responding to promising developments. It also recognizes a hierarchical nature of operations and restoration from basic non-negotiables (core product, service, or expectation) to higher levels of capacity as content evolves. Importantly, this function is not static—it requires regular updating, testing, and integration into decision-making cycles.

National and international standards and guidelines related to broad RM provide frameworks that reflect a growing consensus on best practices aimed at strengthening organizational resilience [2]. According to Tammineedi [3], lack of integrated management standards in business continuity (BC) efforts has historically led to inconsistent and fragmented practices, often producing ineffective and unreliable continuity plans. However, more recent findings by Alharthi and Khalifa [4] show that formalized BC management—guided by recognized standards—can have a positive impact on organizational crisis performance. These standards support cross-disciplinary adoption of integrated systems and strategies that minimize organizational vulnerability, enhance crisis response and recovery, and foster long-term resilience [5,6]. As the complexity of RM increases, an examination of the elements and requirements within and across these standards yields insights that inform and provide a foundation for more effective implementation strategies.

As RM permeates deeper within organizations, it also requires time and resources. Leveraging efforts across RM system implementations can move efforts from coordination to collaboration and then finally to integration of systems for an enterprise. In order to achieve this integrated approach, the contributing systems frameworks must be evaluated for similarities and differences within key elements and across intended outcomes, or aims. This study delves into the application of the major RM system standards used by risk managers to derive a conceptual unified model. Using an organizational toolkit approach, this article compares the frameworks for RM approaches and explores the functional relationships, challenges, and opportunities of integrating RM and business continuity planning (BCP) for resilience. Finally, the study presents a conceptual unified methodology for continuity and resilience that can be applied across broad contexts.

2. Materials and Methods

This study proposes a conceptual unified SRCP approach to manifest organizational resilience by examining widely recognized RM systems and continuity standards aimed at serving the enterprise-level risk manager. Our methodology involved analysis of these standards at framework, functional, and operational levels to determine areas of overlap and gaps that should be addressed to facilitate integrated implementation, as follows:

- Comparative analysis of RM and continuity frameworks set out in the identified standards at the structural framework level.
- Evaluation of the relationship between the identified RM and BC frameworks and their requirements at the functional level.
- Examination of significant operational components of the identified frameworks for system implementation.

The results of our analysis were then combined to derive a conceptual implementation model for a holistic, systems-based approach for risk and continuity planning to serve organizational practitioners.

2.1. Comparative Standards Analysis

In order to determine conceptual alignments, practical overlaps, and implementation gaps, a structured comparison of identified leading standards from the International Organization for Standardization (referred to as ISO), the International Electrotechnical Commission (IEC), and the National Institute of Standards and Technology (NIST) that address different yet related categories of risk was conducted. These standards included the following:

- ISO 31000 (Risk Management) [7];
- ISO 45001 (Occupational Health and Safety) [8];
- ISO 14001 (Environmental Management) [9];
- ISO 22301 (Business Continuity) [10];
- ISO/IEC 27031 [11] and NIST 800 series (Information and Data Security) [12];
- ISO 37101 (Sustainable Community Development) [13].

Each standard was evaluated along several dimensions: general risk definition, scope and applicability, risk treatment mechanisms, and performance measurement approaches. While each standard provides valuable guidance within its domain, no single standard alone provides for comprehensive resilience. For example, ISO 31000 emphasizes enterprise risk treatment, ISO 22301 focuses on BCP, and ISO 27031 emphasizes IT readiness and information and communication technology (ICT). Further, the approach for operational controls and measurement mechanisms differs significantly among the standards, and these differences must be addressed when applying a unified, integrated approach.

This gap analysis demonstrated that while all standards address uncertainty and likelihood associated with risk, only ISO 22301 and ISO/IEC 27031 embed continuity-specific testing, exercise cycles, and recovery-focused performance indicators. Continuity-specific standards (e.g., ISO 22301) include scenario testing and iterative exercises, which are less emphasized in general RM standards. While environmental, health, and safety standards (e.g., ISO 14001 and 45001) include some requirements for periodic testing of response plans and capabilities, these are somewhat limited in scope. This finding reinforces the need for an integrated SRCP approach that draws on multiple frameworks while treating operational gaps. Since manifestations of risk to BC are a function of operational gaps and lack of preparedness and controls, RM must ultimately operate within the broader domain of BC, with a measure of foresight, focusing on integration of core components.

Figure 1 [7–13] below synthesizes this baseline comparison, showing the focus of each standard, how these standards define risk, scope of application, and mechanisms for control and performance measurement, and builds upon the work of Schneider et al. [14]. Describing the guiding elements of each standard shows the functional gaps between the standards, illustrating the details that must be managed in an integrated implementation.

Risk Based Standards	Focus	General Risk Definition	Risk Scope	Operational Controls & Performance Measurement
ISO 31000:2018 Risk Management	Internal focus: within operations and organizations	"effect of uncertainty on objectives" *Commonly expressed in terms of sources of risk, potential events, consequences, & their likelihood	Management of risk faced by organizations in relation to achieving objectives	Develop risk treatment plans to control risks; Establish Indicators for monitoring performance and effectiveness of the risk management framework
ISO 45001: 2018 Occupational Health & Safety		Combination of likelihood of work-related hazardous events or exposures and & severity of related injury or illness	Prevention of injury, ill-health & noncompliance; Mitigation of OHS issues that pose risk to the organization	Develop objectives and plan to control OHS risk and manage associated organizational risks and opportunities; Indicators align with objectives; Audit system
ISO 14001:2015 Environmental Management		"potential adverse effects (threats)" *part of a defined concept of risks and opportunities *Can be expressed as combination consequences of an event and likelihood of occurrence	Prevention of pollution; environmental protection & noncompliance; Mitigation of environmental issues that pose risk to the organization	Develop objectives and plan to control environmental aspects/impacts and manage associated organizational risks and opportunities; Indicators align with objectives; Audit system
ISO 22301:2019 Business Continuity		"effect of uncertainty on objectives" *Can be expressed as combination consequences of an event and likelihood of occurrence	Mitigation of business impacts from events; Legal compliance	Develop objectives and & plan for responding to disturbances; Indicators align with objectives; Perform exercises and tests to evaluate adequacy of plans; Audit system
ISO/IEC 27031:2025 Information Security	Internal and external focus: within operations, organizations and supply chain	"effect of uncertainty on objectives" *Can be expressed as combination consequences of an event and likelihood of occurrence	Events and incidents that could have an impact on ICT infrastructure & systems	Develop objectives and plans to control risk, respond to ICT disturbance; Indicators align with objectives; Perform exercises & tests to evaluate adequacy of plans; Audit system
NIST 800/RMF Data Security		"A measure of the extent to which an entity is threatened by a potential circumstance or event" *typically a function of adverse impact of a potential circumstance or event and the likelihood of occurrence."	Cybersecurity events related to information systems and assets	Develop controls, including types of procedures and training; Indicators for monitoring information systems and assets for cybersecurity events and verify control effectiveness
ISO 37101:2016 Community Sustainable Development	Across communities	"effect of uncertainty on objectives" *Can be expressed as combination consequences of an event and likelihood of occurrence	Mitigation of risk related to environmental and socioeconomic issues in communities; Resilience and sustainable development	Develop objectives and plan for addressing risks and opportunities for community resilience; Indicators align with the 6 purposes and 13 issues; Audit system

Figure 1. Risk-based standards comparison (adapted from Schneider et al. [14]). The asterisks indicate clarification for defined terms derived from the notes to entry provided in the standards.

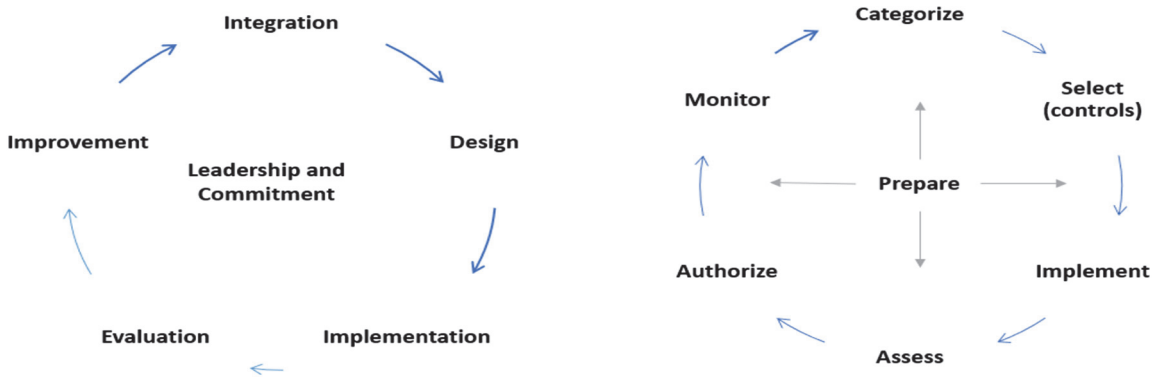
2.1.1. Risk Management Systems Frameworks, Styles, and Language

Disciplinary standards have overlapping but varied and sometimes inconsistent elements or requirements, such as differences in concepts and terminology, documentation formats, and compliance timelines. An examination of a subset of these standards at the framework level provided insight into framing and style differences across these standards that can manifest in implementation of differences in practice. While all of these standards involve RM to some extent, ISO 14001, ISO 37101, ISO 45001, ISO/IEC 27031, and NIST SP-800 provide requirements and guidance for RM in specific disciplines. The evaluation included the broader framework standards, ISO 31000 and ISO 22301, and the NIST Risk Management Framework (RMF) due to its differences in style and perspective from the ISO and IEC approaches. As ISO 22301 follows the same ISO Harmonized Structure as the

discipline-specific ISO management systems standards (MSS), the structure for these other standards is largely captured at the framework level in ISO 22301's approach.

The ISO 31000 standard provides an internationally recognized framework for RM, focused on integrating RM in all aspects of an organization's activities, from strategic planning to operations. The framework can be adapted and built upon to suit an organization's specific needs and context. While ISO 31000 is not an MSS, it is recognized as a key standard for RM and is applied to or referenced in ISO's MSSs. The framework specifies five iterative elements: integration, design, implementation, evaluation, and improvement [7]. In addition, ISO 31000 highlights leadership and commitment in the organization in connection with the framework elements.

NIST's RMF [12] is more specifically focused on RM for information security through categorizing the system, and selecting, implementing, assessing, authorizing, and monitoring controls within information systems. Notably, NIST also includes a preparation step designed to implement essential activities to help prepare the organization to manage its risks using the RMF. Figure 2 summarizes the major elements of the ISO 31000 RMF and the NIST RMF for information systems, adapted from ISO 31000 [7] and the NIST RMF [12].



(**a**) **ISO 31000 RMF** (**b**) **NIST RMF**

Figure 2. Elements of (**a**) the ISO 31000 Risk Management Framework (adapted from [7]) and (**b**) the NIST Risk Management Framework for information systems and organizations (adapted from [12]). Blue arrows indicate the logical progression of elements and the cyclical approach embedded in the two frameworks.

On the surface, these inconsistencies could prevent an integrated approach, given the apparent conflicts. However, these seeming conflicts and gaps can be analyzed and leveraged to create a stronger, unified implementation.

2.1.2. BC Management Framework

ISO 22301 provides an internationally recognized framework for organizations to minimize adverse impacts of disruptions and to ensure they can recover and resume critical business functions and operations quickly when disruptions occur, using a risk-based approach. ISO management systems standards follow a harmonized structure that provides a framework for RM consistent with the Plan-Do-Check-Act (PDCA) model attributed to Shewhart and popularized by W. Edwards Deming. Each standard includes seven broad elements aimed at managing risk in a specific discipline, including context of the organization, leadership, planning, support, operation, performance evaluation, and improvement [15]. The ISO 22301 management system standard for BC is no exception to this rule, but the continuity-specific elements are primarily embedded in the "operation" clause, which generally corresponds to the implementation phase in ISO 31000's RMF. Figure 3 below illustrates the ISO 22301 framework for business continuity.

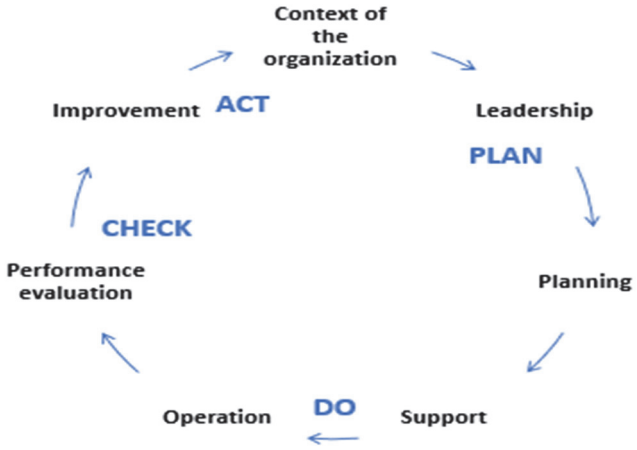


Figure 3. Elements of the ISO 22301 framework. Blue arrows indicate the logical progression of elements and the cyclical approach embedded in the frameworks. The Plan-Do-Check-Act steps are shown in blue and situated within the framework according to their association with the elements of ISO 22301.

Key similarities and differences can be observed across the frameworks examined. As indicated in Figures 2 and 3, RM and continuity frameworks take an iterative approach that involves some form of preparation or planning, implementation of the framework, evaluation or assessment of actions and solutions implemented and their effectiveness, and decisions and actions for improvement. On the other hand, the NIST framework adds specific emphasis on preparing the foundation for implementing the framework, while both ISO standards emphasize leadership. ISO 31000 includes an integration element, and ISO 27301 includes a support element, neither of which is identified at the framework level in the NIST RMF. The NIST RMF incorporates a seemingly unique emphasis on authorization and monitoring. A closer look into the elements of each framework and what they comprise provides further depth on similarities, differences, and opportunities for integration despite the variations in framework structures and terminology.

2.2. Functional Interdependencies of Broadly Applied RM and BC Frameworks

Functional similarities and interdependencies between RM-related standards and continuity frameworks can provide insights into key areas for integration. RM and BC systems serve complementary but often disjointed functions. RM is typically prevention-focused, while continuity planning is both prevention- and resumption-focused. In practice, these functions are interdependent: effective RM reduces the likelihood of disruptive events, while robust continuity (i.e., resilience) reduces the risk of undesirable consequences [1] and ensures functionality in the face of residual risks.

2.2.1. RM Standards

Tables 1 and 2 indicate the core elements required for implementation of the ISO 31000 and NIST RM frameworks, illustrating the similar yet different implementation guidance therein. Comprehending these nuances can guide holistic implementation. As noted in Section 2.1, the ISO 31000 framework specifies five iterative elements: integration, design, implementation, evaluation, and improvement, as well as an overarching element associated with leadership and commitment [7]. These elements are described at the functional level in Table 1, below, based on content analysis of the ISO 31000 RMF.

While the terminology and perspective set out in the NIST RMF are notably different from those of ISO 31000, including its scope in relation to information systems, closer examination at the functional level revealed additional similarities in relation to monitoring the effectiveness of systems and controls, as well as preparing for implementation of the

RMF. Notably, NIST calls for a 'prepare' step that delineates context and priorities that reflect organizational environments and needs. For the most part, this is embedded in the 'design' element of ISO 31000's RMF, but NIST's emphasis on putting the necessary resources and foundations in place at the start to support execution of RM from an organization-level and system-level perspective is a key component for both RM and resilience efforts. The NIST RMF elements are described below in Table 2, based on content analysis of the framework.

Table 1. Functional description of elements of the ISO 31000 risk management framework (adapted from [7]).

ISO 31000 RMF Element	Functional Description
Integration	Integrate RM in organizational governance, responsibilities, strategy, objectives, and operations to the extent necessary to reach desired performance levels and achieve long-term viability.
Design	Design the RMF based on the organization's internal and external context, including stakeholder needs and expectations. Assign roles, responsibilities, and accountabilities; allocate resources for RM. Establish an approach for communication and consultation to support the RMF and "facilitate the effective application of" RM.
Implementation	Implement the RMF through RM planning, decision-making processes, and responsibilities. Ensure the organization's procedures, processes, and other arrangements for RM are understood and practiced.
Evaluation	Evaluate the effectiveness of the RMF by periodically measuring framework performance against the organization's purpose, implementation plans, indicators, and expected behaviors, and determine whether it remains suitable to support achievement of the organization's objectives.
Improvement	Ensure improvement by monitoring and adapting the RMF to address internal and external changes, identified gaps, and opportunities for improvement.
Leadership and Commitment	Demonstrate leadership and commitment by adapting and implementing the framework, establishing and disseminating an RM plan, allocating necessary resources, and assigning responsibilities, authorities, and accountabilities for RM within the organization.

Table 2. Functional description of elements of the NIST risk management framework for information systems and organizations (adapted from [12]).

NIST RMF Element	Functional Description
Prepare	Prepare to execute the RMF from an organization- and system-level perspective, by establishing a context and priorities for managing risk.
Categorize	Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
Select	Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on RA.
Implement	Implement the controls and describe how the controls are employed within the system and its environment of operation.
Assess	Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
Authorize	Authorize the system or its common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the organization itself is acceptable.
Monitor	Monitor the system and associated controls on an ongoing basis, assess control effectiveness, document changes to the system and environment of operation, conduct RAs and impact analyses, and report on the security and privacy posture of the system.

2.2.2. Business Continuity Management Standards

ISO 22301 remains the guiding standard for business continuity management (BCM) and is aimed at organizations of any sector, size, or geographic location. It defines continuity

as an organizational capability to continue the delivery of products or services at acceptable predefined levels following a disruptive incident. The standard emphasizes a lifecycle approach that includes impact assessment, continuity planning, testing, and continuous improvement [16].

The primary function of BCM is to develop a robust and sturdy framework for organizational resilience [16]. BC managers can collaborate with all-hazards practitioners, such as those involved in RM, disaster recovery, crisis management, and emergency response, to develop proactive business continuity plans (BCP); however, these plans are broader than hazard-based planning and serve continuous improvement. BC encompasses resources, actions, procedures, and other information designed to prepare organizations for maintaining essential functions during major organizational disruptions or disasters [17].

The Business Continuity Management System (BCMS) framework [10] incorporates business impact analysis (BIA) as well as assessment of the risks of disruption to the organization's prioritized activities and to their required resources, following the process outlined in ISO 31000, in order to determine BC priorities and requirements. In contrast, the BCMS framework also includes the following:

- Identification and selection of continuity strategies and solutions that consider options for before, during, and after disruption;
- Implementation of solutions, plans, and procedures as part of a response structure to activate BC solutions when disruption occurs, including plans and procedures to guide and inform response and recovery efforts;
- BCP to address identified risks and opportunities, including necessary communication processes and recovery processes;
- Testing and exercising to validate the effectiveness of BC strategy and solutions;
- Evaluation of adequacy and effectiveness of BIA, RA, strategies, solutions, plans, and procedures, including BC capabilities of relevant partners and external providers [10].

The elements of the ISO 22301 BCMS framework are mapped to a PDCA structure and described below in Figure 4, with critical differences between the BCMS elements and those of the other identified RM standards shown in blue within each step, based on our comparative analysis.

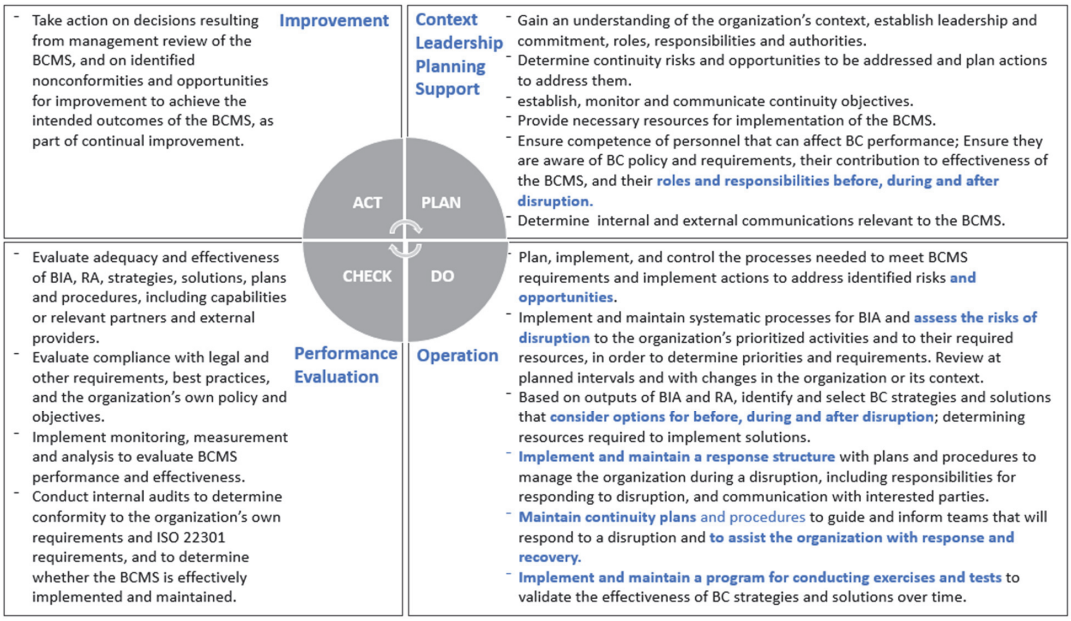


Figure 4. Elements of the ISO business continuity risk management framework. Critical differences between the BCMS elements and elements of other RM standards are shown in blue within each step. The arrows indicate the cyclical nature of a PDCA approach.

As shown in Tables 1 and 2 and Figure 4, there are numerous similarities across risk management frameworks. In particular, all of the frameworks include components related to putting the foundation in place for implementation, including gaining an understanding of the organization's internal and external context, management, leadership, and support, and the necessary competencies for implementing the frameworks. However, the NIST RMF elevates the importance of preparing this foundation to the framework level as its own element.

All frameworks examined involve RA and planning from a preventative perspective, including strategies and actions to address identified risks, the use of performance indicators with monitoring and evaluation to gauge the effectiveness of strategies and actions, and feedback loops or mechanisms to support improvement over time. Yet the continuity framework goes beyond a focus on risk as a threat to include opportunities, or potentially beneficial impacts on the organization, and is aimed also at resumption of operations after disruption. An integrated SRCP will need to incorporate these factors to enhance organizational resilience.

2.2.3. Assessing and Responding to System Critical Impacts

Continuity planning is an integral part of BCM, and identifying mission-critical operations is a core element. Continuity planning begins with risk identification, including threats, and then proceeds towards managing the risks within the business recovery timeline, creating an environment for risk reduction. As the BCP is created, testing criteria and procedures are developed. These essential functions anchor business resumption strategies and inform prioritization during crises. Criteria for determining criticality include data quality [18], revenue implications, regulatory compliance, customer impact, and interdependency with other organizational units. Organizational charts, dependency matrices, and needs assessments are tools to support this analysis [19]. Effective continuity planning also requires an understanding of internal and external resource flows. Resources include personnel, facilities, data systems, communication equipment, and supply chains [20]. Logistics—ensuring the right resources are available in the right place at the right time—is a critical enabler of continuity. Continuity is as much a logistical challenge as a strategic one, especially in organizations that rely on just-in-time delivery or geographically distributed teams [21].

Realizing continuity and creating resilience means that each risk and vulnerability must be assessed for not only individualized impact but also for interdependent 'ripple effects' and movement [22,23]. In this way, risk can then be prioritized by the organization in two ways: first, for its centrality to core function and output, and second, for its comprehensive impact on the organization, another form of dependency and extended vulnerability [6]. Continuity extends to resilience when impacts can be recast as opportunities or shifts or pivots for robustness and growth, sometimes known as the positive portion of a SWOT (strengths–weaknesses–opportunities–threats) strategic analysis.

The organization's prioritized exposures support selection and development for contingency responses that include options for before, during, and after disruptions. ISO 22301 discusses the need for effective strategies and solutions to manage identified and prioritized disruptions. Contingencies should reduce the likelihood, impact, and period of disruption, as well as meet recovery time frames, protect prioritized activities, and ensure adequate resources are available. Contingencies are not meant to eliminate every possible risk; in fact, organizations have finite resources, and consideration must be given to the costs and benefits of various mitigation strategies. When determining these, it is important to include many resource costs/benefits, such as those to human capital, physical infrastructure, information/data, logistics, as well as finances.

2.3. Examination of Significant Operational Components for Integrated SRCP

An integrated SRCP requires evaluation of cross-system functions as well as embedded components. This allows an implementer to leverage actions for greater effectiveness. As RM and continuity planning combine, the cross-functional capacities that engage stakeholders in the process are literally what holds the system together. To transition to a fully functional SRCP, organizations must engage those who operate the system and benefit from it, including stakeholders, and respond to feedback to continuously improve. Testing the plan through exercises, reviewing it in light of new threats or organizational changes, and updating it regularly to reflect lessons learned ensures effectiveness over time.

2.3.1. Critical Communications

Critical communication is the process by which organizations manage the flow of information during disruptions and high-intensity operations like those within a resumption process. It supports internal coordination, protects external trust, and enables timely decision-making under adverse conditions. Without effective communication, even technically sound resumption and resilience can fail due to confusion, misinformation, or reputational harm. High-quality critical communication provides the structure for ensuring that accurate and relevant information reaches the right stakeholders at the right time. Internally, it supports operational coherence among staff, leadership, and partners. Externally, it ensures that customers, regulators, suppliers, and the public are informed and engaged, which is necessary to sustain continuity and maintain institutional credibility during and after a crisis [24].

In complex organizational systems facing disruptions, critical communication functions as an essential subsystem that governs the flow of information during high-impact incidents and resumption activities. Effective communication facilitates dynamic coordination across internal units and external stakeholders, enabling adaptive decision-making and maintaining trust under conditions of uncertainty and time pressure. Without reliable communication that is clear, accurate, and timely, even the best systems fold due to information asymmetries, operational misalignment, or loss of stakeholder confidence [25,26].

From a systems perspective, communication serves both as a control mechanism and as an enabling process, ensuring feedback loops function effectively within the larger resilience framework. Internally, communication synchronizes operational activities among staff, leadership, and partners, supporting coherent execution of recovery procedures. Externally, it preserves system legitimacy by engaging customers, regulators, suppliers, and the public, thereby sustaining the social license to operate amid disruption [27,28]. Designing this subsystem involves clearly specified activation protocols, defined communication roles, and standardized procedures for message development and dissemination. A dedicated communication node—comprising cross-functional team members with explicitly delineated responsibilities—acts as an integrative hub that consolidates situational data, crafts stakeholder-relevant messages, and manages interaction channels [29,30]. Leveraging pre-approved communication templates enables rapid, consistent messaging that addresses critical informational components: event context, affected populations, expected recovery timelines, and recommended protective measures [31].

Given the potential for disrupted traditional communication pathways during crises, the subsystem must incorporate resilient, redundant channels and ensure a comprehensive understanding of communication protocols across the organizational hierarchy. This entails regular training in media relations and social media governance, as well as maintaining up-to-date and accessible contact databases spanning employees, regulatory bodies, emergency services, vendors, and media outlets [27,29,32]. Supporting documentation—such as checklists, media engagement policies, message templates, and communication logs—constitutes

an operational knowledge base that anchors execution under pressure and mitigates risks of message fragmentation or delay. From a systemic viewpoint, these artifacts function as standardized interfaces that maintain communication coherence and traceability throughout crisis response phases [33]. Integrating crisis communication seamlessly into the organizational continuity system transforms it from an ancillary function into a strategic capability that strengthens resilience at multiple levels. By enhancing information flow control, reducing uncertainty, and reinforcing stakeholder confidence, communication supports the adaptive capacity and robustness necessary for organizations to thrive within volatile and high-risk environments [26,34].

2.3.2. Training, Testing, and Exercises

Training and exercises are essential to the effective implementation of any continuity or emergency response plan. Even the most technically sound plans cannot be operationalized without personnel who are familiar with their roles, the procedures they must follow, and the systems they must coordinate. Comprehensive and recurring training ensures that teams are prepared not only to execute their responsibilities under pressure but also to adapt to dynamic conditions during a disruption [35]. Effective training is actionable practice. This effort is the operational step that transforms continuity and emergency response plans from conceptual frameworks into implementable, effective systems. Simply, plans remain inadequate unless personnel are practiced in their designated roles, procedures, and supporting systems [36]. Systematic, recurrent training equips teams with the skills to not only execute responsibilities under tough conditions but also to recognize and adapt to evolving conditions during disruptions [37,38].

Targeted training should be provided for all personnel assigned to emergency response, BC, and crisis communication functions to create the ability to perform with organizational expectations and within operational parameters [39]. Leadership training results in effective cross-functional coordination and evidence-based decision-making [40,41]. General training that focuses both on standards and strategy, a combination of life safety procedures, information sharing, and capacity building for all staff members [35] can build resilience. Such alignment facilitates compliance and organizational readiness.

Training is not complete without testing and evaluation, assessing the timeliness, feasibility, and operability of continuity and emergency plans [36]. Exercises validate plans, identify procedural and coordination gaps, and facilitate cross-collaboration. Exercise typologies span the spectrum from simple walkthroughs and notification drills to comprehensive functional and full-scale simulations [42]. Tabletop exercises drive scenario-based discussion among team members, allowing participants to clarify roles and anticipated actions within a low-risk environment [42]. Functional exercises simulate testing communication flows, resource mobilization, and tactical decision-making. The design of the exercises is informed by organizational RA and continuity planning priorities, ensuring scenario selection and complexity are relevant and scalable [42]. As organizational preparedness matures, integrating exercises with external partners, including emergency management agencies or critical resources, develops interoperability and shared situational awareness [41]. System adaptation and continuous improvement come through the post-exercise evaluation process. Structured after-action reviews and participant debriefings capture successes, challenges, and required corrective actions [37]. Lessons learned drive updates to plans, protocols, and training curricula [35]. By institutionalizing a continuous cycle of training, testing, evaluation, and refinement, organizations build dynamic adaptive capacity and resilience. This evolves continuity planning from a compliance-driven formality into a core operational process embedded in organizational culture and resilience strategy [42].

3. Results

In any management system standard, words matter. Definitions and frameworks become guiding ideals for implementation. Thus, this study examined the standards with regard to terminology, definitions, framing, and expectations. As organizations strive to manifest robust and efficient RM, leaders should be looking to leverage efforts that seem to have similar aims. At least, coordination of RM provides coherence across the systems. Organizations are certainly free to implement standalone systems; however, integration can also provide a matrixed effort with more robust connections, outcomes, and visible responsibility. Gaps and inconsistencies can either become insurmountable or create an opportunity for dialogue, choice, and leadership prioritization.

Implementation of an effective SRCP depends on leadership support for resourcing, prioritization (especially when there is no crisis), and broad integration. Manifesting resilience requires more than just identifying threats or mapping operational impacts—it requires an integrated analytical model that combines RA and BIA with cross-functional components into a unified management-driven decision-making framework. The key difference between the two BC tools (BIA and RA) is that Business Impact Analysis (BIA) does not directly focus on the likelihood of events; rather, it assumes worst-case scenarios. Business Impact Analysis can be conducted unescorted by a formal RA, but RA in an organization cannot realistically occur in most cases without some form of BIA. BIA does not directly address identified risks, but BIA-determined criticality and sensitivity of a system influence RM requirements and can thus be a catalyst for risk prioritization and mitigation. Quinn et al. ([43], p. 13) maintain that BIA serves as a "nexus for understanding risk". It also enables a broader understanding of system impacts [44] in an organization. An organization should incorporate BIA in RA to quantify and prioritize the risks it identifies. The two tools are synergistic: BIAs help prioritize functions based on criticality, while RAs inform mitigation strategies based on threat exposure. Sequencing RA and BIA enables the accurate identification of threats and their organizational impacts. When conducted iteratively and integrated into broader continuity planning, these tools enable organizations to map vulnerabilities, identify recovery time objectives, and allocate resources more effectively.

Conversely, RA provides a forward-looking lens through which potential threats are identified, evaluated, and prioritized [45]. It involves systematically assessing hazards—natural or man-made—and understanding their potential consequences on critical operations. Typically, RA outputs include a categorized list of risks ranked by likelihood and severity, with common categories such as infrastructure failure, loss of facility or access, data breaches, personnel shortages, and broader cascading disruptions. BIA shifts the focus from external threats to internal operational consequences, enabling organizations to evaluate the impact of disruptions in terms of recovery time, data tolerance, regulatory compliance, and reputation. The effort focuses evaluation on downstream impacts to inform actions. For each risk, recovery timeframes for specific functions, expected level of service, and resources are required. Thus, it forces an organization to define core operations in times of stress [45].

Feedback loops are important. RAs that focus on assets and critical functions support the BIA process, helping to identify dependencies, recovery points, and resource gaps. In turn, BIA findings can refine RA efforts by highlighting which risks require mitigation due to the strategic importance of the affected functions. This ensures smarter investment in controls, aligning expenditures to operational priorities [46]. Integration also supports worst-case scenario planning. Rather than simply listing risks or estimating impact in isolation, organizations can use the combined analysis to simulate multi-nodal or exacerbated crises—such as cyberattacks that compromise both data and personnel workflows—to form continuity strategies that are agile, layered, and responsive to actual business needs.

Integrated Model for Organizational Continuity and Resilience

Below, we propose an integrated model to support continuity and resilience as a system-wide function within risk-prone environments. Key areas for integration were found based on observed functional interdependencies between RM-related standards and continuity frameworks. While functionally disjointed, BC and risk systems present as complementary functions: RM is typically prevention-focused [1], while continuity planning is both prevention- and resumption-focused.

Creation of an integrated SRCP model to support organizational continuity and resilience reflects the interrelationships, inputs, and outputs [6] examined in this methodology. As illustrated below in Figure 5, a generic integrated model is possible as a holistic framework for continuity and resilience upon which virtually any organization can build, regardless of its size, sector, or compliance environment. The resulting model serves as a holistic map of how all of the components work together in a system—the dynamic interactions and feedback loops connect inputs and outputs across the system environment [47,48]. Since risk itself is dynamic in multiple ways, variable in time, scale, and substance, so too must the systems that manage it. The model considers functionality and context-driven capacities that can be applied across broad typologies of organizations, with adjustments that reflect behavior, need, and context. Our derivation considered all of these factors in the proposed model. It represents a distillation and integration of key functional and operational requirements found in the identified standards, mapped to a PDCA framework, as shown in Figure 5.

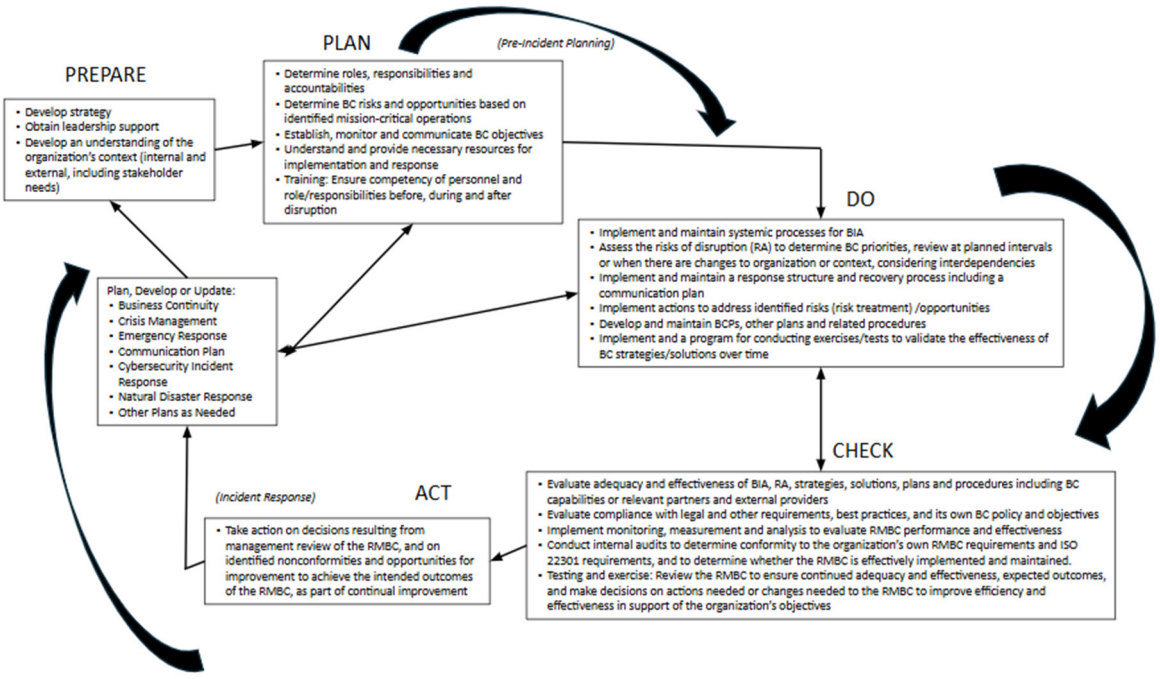


Figure 5. SRCP unified model to support organizational continuity and resilience.

4. Discussion

Consistent with Aven [1], our analysis suggests that risk and resilience management should not be viewed as independent or separate management functions, but rather they are—or should be—considered as an integrated part of the risk field. A comprehensive approach to risk analysis and management—one that incorporates systems thinking, continuity, and resilience—is essential for developing the knowledge, strategies, and decision-making capabilities needed to manage limited resources effectively. This reinforces the

value of an integrated SRCP approach that addresses operational vulnerabilities through alignment of multiple frameworks.

While RM standards can be very useful to help organizations respond to risk, this examination suggests there are limitations for organizational resilience when focusing on RM alone. The analysis of the related standard frameworks suggests alignment in many areas despite variations in terminology and format, as well as some critical gaps that could be addressed with an integrated SRCP approach that draws on multiple frameworks. Specifically, this includes preparing the organizational and resource foundations for implementing an integrated SRCP approach. While many system standards display alignment across many areas—despite differences in terminology and format—they also exhibit critical gaps. These limitations may be addressed through an integrated SRCP approach that draws from multiple frameworks to strengthen organizational preparedness and response, recognizing that implementation remains unique and must be built upon by the organization to meet its specific needs and within its distinct context.

4.1. Integration of BIA and RA in SRCP

One of the model's strengths lies in its ability to facilitate evaluation of cross-system functions and embedded components. This enables implementers to coordinate actions more effectively and leverage system interdependencies to enhance performance. A key area of functional integration within this approach involves the BIA and RA. The greatest benefit can occur when these tools are applied iteratively and interactively, rather than sequentially or siloed [44]. For example, conducting an RA may highlight that a regional flood has a low probability but could cause severe infrastructure failure. A concurrent BIA would reveal whether a data center in that location supports time-sensitive services—and whether even a brief outage could violate service-level agreements or trigger financial penalties. The integrated SRCP lens ensures that risks are not just cataloged but prioritized based on their business-critical impacts. Figure 6 illustrates the opportunities and potential benefits of an integrated approach for RA and BIA, as part of an integrated SRCP model.

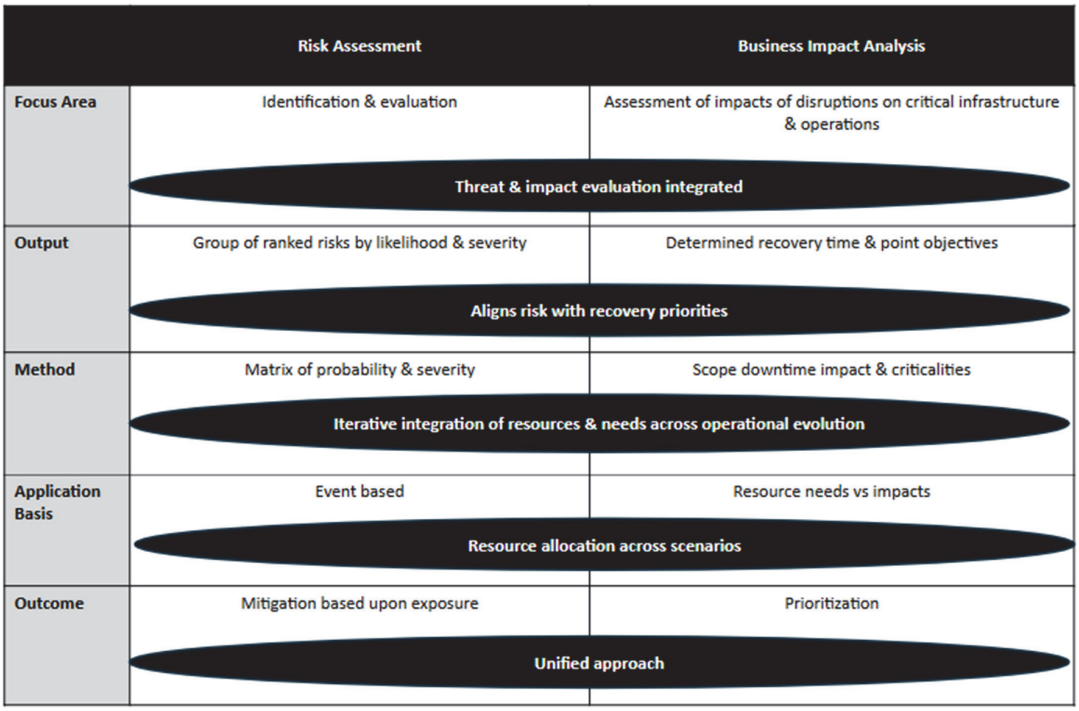


Figure 6. Benefits of integrated BIA:RA as part of an integrated SRCP model.

4.2. Model Applicability, Implementation, and Effectiveness

Importantly, sectoral differences (e.g., healthcare vs. manufacturing vs. finance) might necessitate unique adaptations of the SRCP model. For instance, regulatory constraints, critical resource dependencies, and tolerance for downtime vary widely across industries, driven by the unique environments/contexts that these organizations face. These unique circumstances drive resilience capacity, reflecting vulnerabilities and exposures. Each organization must consider these, whether implementing each risk management system or integrating them in an SCRP mode.

Ultimately, BC outcomes are shaped by systemic gaps and organizational preparedness. RM, therefore, must function within a wider continuity and preparedness domain, guided by strategic foresight and grounded in integrated planning. Importantly, the integrated SRCP model that is proposed provides assurance that organizations at all levels can effectively plan, respond to, and manage disruptions of various forms and use that leverage to drive organizational resilience. The integrated framework provides for an effective, systems-based approach: identifying threats, assessing organizational vulnerabilities, mapping dependencies, and establishing recovery priorities. System-driven integration provides a comprehensive map of not only what could go wrong, but also what must go right—and how quickly. This combined approach transforms the territory of continuity planning from a compliance exercise into a strategic asset, supporting informed risk-taking, agile recovery, and evaluation and pursuit of future opportunities, resulting in longer-term resilience.

Traditional RA methodologies—typically grounded in probability estimates and impact likelihoods—are no longer sufficient in the face of rising uncertainty and system fragility. As Aven [1] argues, these models are particularly inadequate for complex systems with high exposure to unknown or emergent risks. In contrast, the framework proposed in the SRCP approach can enable planning for service degradation, partial functionality, and staged recovery, driving responsiveness to new developments while supporting restoration from core system functions to full operational capacity. It also recognizes a hierarchical nature of operations for restoration from basic non-negotiables (core product, service, or expectation) to higher levels of capacity as the context evolves.

The SRCP model cultivates an organization-specific strategy, embedding a forward-thinking, future-casting ideology in their systems as they navigate uncertainty in a risky and brittle world. Crucially, the SRCP model is dynamic. It requires continuous updating, rigorous testing, and integration into routine decision-making. This ensures it remains responsive to organizational changes and emerging landscapes, an effective system that adapts to suit the organization's particular purpose, context, and needs as well as the expectations of its stakeholders.

4.3. Direction for Future Research

Future research on integrated systems for risk, continuity, and resilience is needed to explore the origin of gaps that may be encountered when integrating risk and continuity framework elements. This paper derived a conceptual integrated model through examination of terminology, definitions, and framing. While inconsistencies in these specifics could prevent an integrated approach, this model proposes that these conflicts and gaps can be used to create a stronger, unified implementation. Future work is needed to evaluate the strengths and weaknesses of multiple single-system implementations versus the integrated approach, including measures of efficacy, as well as future research to provide a structured method for prioritizing actions when faced with constraints that prevent the proposed implementation.

Further, an integrated approach supposes that the implementers possess the technical capacity for this broad work. Aven [1] suggests that integrating risk and resilience may expose gaps in technical competencies necessary for contextual RA that adequately serve continuity and resilience. Thus, this proposed SRCP model also relies on the capacity of those who implement it, as well as human and organizational dynamics.

It is a formidable exercise to understand, scope, and assess detailed and domain-specific organizational risks, let alone the expansive and often interconnected risks across today's organizations. The intent of this paper was to propose an integrated framework to support organizational continuity and resilience that addresses the question "What must continue, no matter what?" coupled with "what operations and outputs grow our opportunities?" Our model aims to serve as a roadmap for practitioners to respond to these questions and streamline an integrated implementation of RM and BIA across disciplines.

All risks reflect their origin, and as our world becomes more complex, so do the systems that manage it. The complicated challenges facing modern organizations demand both risk-based and resilience-informed thinking to generate enduring solutions.

Author Contributions: Conceptualization, D.H. and J.S.; methodology, J.S.; validation, L.L.G. and J.S.; formal analysis, L.L.G., D.H. and J.S.; investigation, J.S., D.H. and L.L.G.; resources, J.S., L.L.G. and D.H.; data curation, L.L.G., D.H. and J.S.; writing—original draft preparation, L.L.G., D.H. and J.S.; writing—review and editing, D.H., L.L.G. and J.S.; visualization, J.S., D.H. and L.L.G.; project administration, J.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

RM	Risk Management
RA	Risk Assessment
IT	Information Technology
SRCP	Systems for Risk and Continuity Planning
BC	Business Continuity
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ICT	Information and Communication Technology
MSS	Management Systems Standard
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
PDCA	Plan-Do-Check-Act
BIA	Business Impact Analysis
BCP	Business Continuity Plan
SWOT	Strengths-Weaknesses-Opportunities-Threats

References

1. Aven, T. The Call for a Shift from Risk to Resilience: What Does It Mean? *Risk Anal.* **2019**, *39*, 1196–1203. [CrossRef]
2. Tiernan, A.; Drennan, L.; Nalau, J.; Onyango, E.; Morrissey, L.; Mackey, B. A Review of Themes in Disaster Resilience Literature and International Practice since 2012. *Policy Des. Pract.* **2019**, *2*, 53–74. [CrossRef]
3. Tammineedi, R.L. Business Continuity Management: A Standards-Based Approach. *Inf. Secur. J. Glob. Perspect.* **2010**, *19*, 36–50. [CrossRef]

4. Alharthi, M.N.A.N.; Khalifa, G.S.A. Business Continuity Management and Crisis Leadership: An Approach to Re-Engineer Crisis Performance within Abu Dhabi Governmental Entities. *Int. J. Emerg. Technol.* **2019**, *10*, 32–40.
5. Galaitsi, S.E.; Pinigina, E.; Keisler, J.M.; Pescaroli, G.; Keenan, J.M.; Linkov, I. Business Continuity Management, Operational Resilience, and Organizational Resilience: Commonalities, Distinctions, and Synthesis. *Int. J. Disaster Risk Sci.* **2023**, *14*, 713–721. [CrossRef]
6. Berkes, F. Understanding Uncertainty and Reducing Vulnerability: Lessons from Resilience Thinking. *Nat. Hazards* **2007**, *41*, 283–295. [CrossRef]
7. *ISO 31000: 2018*; Risk Management—Guidelines. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 16 July 2025).
8. *ISO 45001:2018*; Occupational Health and Safety Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/63787.html (accessed on 22 July 2025).
9. *ISO 14001:2015*; Environmental Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2015. Available online: https://www.iso.org/standard/60857.html (accessed on 22 July 2025).
10. *ISO 22301:2019*; Security and Resilience—Business Continuity Management Systems—Requirements. ISO: Geneva, Switzerland, 2019. Available online: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en (accessed on 22 July 2025).
11. *ISO/IEC 27031:2025*; Cybersecurity-Information and Communication Technology Readiness for Business Continuity. ISO: Geneva, Switzerland, 2025. Available online: https://www.iso.org/standard/27031 (accessed on 22 July 2025).
12. NIST/Joint Task Force Transformation Initiative. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018; NIST SP 800-37r2. [CrossRef]
13. *ISO 37101:2016*; Sustainable Development in Communities—Management System for Sustainable Development—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2016.
14. Schneider, J.; Romanowski, C.; Mishra, S.; Raj, R.K.; Dobie, S. Building Robust Risk Management as a Method of Situational Awareness at the Local Level. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018; pp. 1–7. [CrossRef]
15. ISO. *Harmonized Structure for MSS with Guidance for Use, Annex SL in ISO/IEC Directives, Part 1*; ISO: Geneva, Switzerland, 2024. Available online: https://www.iso.org/sites/directives/current/consolidated/index.html#_Toc165304996 (accessed on 16 July 2025).
16. Steen, R.; Haug, O.J.; Patriarca, R. Business Continuity and Resilience Management: A Conceptual Framework. *J. Contingencies Crisis Manag.* **2024**, *32*, e12501. [CrossRef]
17. Skouloudis, A.; Tsalis, T.; Nikolaou, I.; Evangelinos, K.; Leal Filho, W. Small & Medium-Sized Enterprises, Organizational Resilience Capacity and Flash Floods: Insights from a Literature Review. *Sustainability* **2020**, *12*, 7437. [CrossRef]
18. Fisher, C.W.; Kingma, B.R. Criticality of Data Quality as Exemplified in Two Disasters. *Inf. Manag.* **2001**, *39*, 109–116. [CrossRef]
19. Theoharidou, M.; Kotzanikolaou, P.; Gritzalis, D. Risk-based criticality analysis. In *Critical Infrastructure Protection III*; Palmer, C., Shenoi, S., Eds.; Springer: Berlin/Heidelberg Germany, 2009; pp. 35–49. [CrossRef]
20. Barratt, M.; Barratt, R. Exploring Internal and External Supply Chain Linkages: Evidence from the Field. *J. Oper. Manag.* **2011**, *29*, 514–528. [CrossRef]
21. Xu, J.; Huang, H. The Analysis of Logistics Outsourcing Risk: A System Dynamics Approach. In Proceedings of the 2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM), Harbin, China, 9–10 January 2010; Volume 1, pp. 156–159. [CrossRef]
22. Moreno-Baca, F.; Cano-Olivos, P.; Sánchez-Partida, D.; Martínez-Flores, J.-L. The Bullwhip Effect and Ripple Effect with Respect to Supply Chain Resilience: Challenges and Opportunities. *Logistics* **2025**, *9*, 62. [CrossRef]
23. Bhamra, R.; Dani, S.; Burnard, K. Resilience: The Concept, a Literature Review and Future Directions. *Int. J. Prod. Res.* **2011**, *49*, 5375–5393. [CrossRef]
24. Cassling. Six Elements of a Crisis Communication Plan. Available online: https://www.cassling.com/knowledge-center/six-elements-of-a-crisis-communication-plan (accessed on 16 July 2025).
25. Coombs, W.T. The Value of Communication during a Crisis: Insights from Strategic Communication Research. *Bus. Horiz.* **2015**, *58*, 141–148. [CrossRef]
26. Ulmer, R.R.; Sellnow, T.L.; Seeger, M.W. *Effective Crisis Communication: Moving from Crisis to Opportunity*; Sage Publications: Thousand Oaks, CA, USA, 2022; ISBN 1-0718-5239-2.
27. Liu, B.F.; Austin, L.; Jin, Y. How Publics Respond to Crisis Communication Strategies: The Interplay of Information Form and Source. *Public Relat. Rev.* **2011**, *37*, 345–353. [CrossRef]
28. Heath, R.L.; O'Hair, D. *Handbook of Risk and Crisis Communication*; Routledge: New York, NY, USA, 2009; ISBN 0-8058-5777-X.
29. Reynolds, B.; Seeger, M.W. Crisis and Emergency Risk Communication as an Integrative Model. *J. Health Commun.* **2005**, *10*, 43–55. [CrossRef]

30. Seeger, M.W. Best Practices in Crisis Communication: An Expert Panel Process. *J. Appl. Commun. Res.* **2006**, *34*, 232–244. [CrossRef]
31. Fearn-Banks, K.; Kawamoto, K. *Crisis Communications: A Casebook Approach*, 6th ed.; Routledge: New York, NY, USA, 2024; ISBN 978-1-003-01928-2. [CrossRef]
32. Jin, Y.; Liu, B.F.; Austin, L.L. Examining the Role of Social Media in Effective Crisis Management: The Effects of Crisis Origin, Information Form, and Source on Publics' Crisis Responses. *Commun. Res.* **2014**, *41*, 74–94. [CrossRef]
33. Coombs, W.T. *Ongoing Crisis Communication: Planning, Managing, and Responding*; Sage: Thousand Oaks, CA, USA, 2007; ISBN 1-4129-4991-2.
34. Wachtendorf, T.; Kendra, J.M.; DeYoung, S.E. Community Innovation and Disasters. In *Handbook of Disaster Research*; Rodríguez, H., Donner, W., Trainor, J.E., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 387–410, ISBN 978-3-319-63254-4. [CrossRef]
35. Madrigano, J.; Chandra, A.; Costigan, T.; Acosta, J.D. Beyond Disaster Preparedness: Building a Resilience-Oriented Workforce for the Future. *Int. J. Environ. Res. Public Health* **2017**, *14*, 1563. [CrossRef]
36. Hall, C.E.; Wehling, H.; Stansfield, J.; South, J.; Brooks, S.K.; Greenberg, N.; Amlôt, R.; Weston, D. Examining the Role of Community Resilience and Social Capital on Mental Health in Public Health Emergency and Disaster Response: A Scoping Review. *BMC Public Health* **2023**, *23*, 2482. [CrossRef]
37. Smith, T.; Wilson, D.; Jones, D.; Plett, M.; Bates, R.; Veilleux, N. Investigation of Belonging for Engineering and Science Undergraduates by Year in School. In Proceedings of the 2012 ASEE Annual Conference & Exposition, San Antonio, TX, USA, 10–13 June 2012; pp. 25.858.1–25.858.11. [CrossRef]
38. McNeil, C.; Divi, N.; Smolinski, M.S. Looking Ahead in the Rearview Mirror: During Action Review and Tabletop (DART) to Strengthen Health Emergency Readiness and Resiliency. *Disaster Med. Public Health Prep.* **2023**, *17*, e355. [CrossRef]
39. Civča, D.; Atstāja, D.; Koval, V. Business Continuity Plan Testing Methods in an International Company. *Restruct. Manag. Increase Compet. Trading Co Latv.* **2021**, *5*, 341.
40. Boersma, K.; Ferguson, J.; Groenewegen, P.; Wolbers, J. The Dynamics of Power in Disaster Response Networks. *Risk Hazards Crisis Public Policy* **2021**, *12*, 418–433. [CrossRef]
41. Riggio, R.E.; Newstead, T. Crisis Leadership. *Annu. Rev. Organ. Psychol. Organ. Behav.* **2023**, *10*, 201–224. [CrossRef]
42. Boin, A.; Van Eeten, M.J. The Resilient Organization. *Public Manag. Rev.* **2013**, *15*, 429–445. [CrossRef]
43. Quinn, S.; Ivy, N.; Chua, J.; Barrett, M.; Witte, G.; Feldman, L.; Topper, D.; Gardner, R. *Using Business Impact Analysis to Inform Risk Prioritization and Response*; NIST: Gaithersburg, MD, USA, 2022. Available online: https://www.nist.gov/publications/using-business-impact-analysis-inform-risk-prioritization-and-response (accessed on 22 July 2025).
44. Sahebjamnia, N.; Torabi, S.A.; Mansouri, S.A. Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *Eur. J. Oper. Res.* **2015**, *242*, 261–273. [CrossRef]
45. Russo, N.; São Mamede, H.; Reis, L. An Approach to Business Continuity Self-Assessment. *Technologies* **2025**, *13*, 242. [CrossRef]
46. Hassel, H.; Cedergren, A. Integrating Risk Assessment and Business Impact Assessment in the Public Crisis Management Sector. *Int. J. Disaster Risk Reduct.* **2021**, *56*, 102136. [CrossRef]
47. Graham, J.; Kaye, D. *A Risk Management Approach to Business Continuity: Aligning Business Continuity and Corporate Governance*; Rothstein Publishing: Brookfield, CT, USA, 2015; ISBN 1-931332-88-6.
48. Corrales-Estrada, A.M.; Gómez-Santos, L.L.; Bernal-Torres, C.A.; Rodriguez-López, J.E. Sustainability and Resilience Organizational Capabilities to Enhance Business Continuity Management: A Literature Review. *Sustainability* **2021**, *13*, 8196. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.