# Overview of Business Continuity Management Systems (BCMS) and Supply Chain Continuity Management (SCCM) – WORKING PAPER for REVIEW)

**John W. Spink, Ph.D.**

Michigan State University, Assistant Professor, Supply Chain Management Department, Business College, Michigan State University, & Director, Food Fraud Prevention Academy LLC

**Reference:** Spink, J. W. (2024). Chapter – *Overview of business continuity management systems (BCMS) and Supply Chain Continuity Management (SCCM) – Working Paper Supplement.* In ***Supply Chain Management Introduction*** **(2025)**, ISBN##, https://www.SCMintro.com

## Abstract

Business Continuity Management Systems (BCMS) provide a comprehensive organizational framework designed to ensure that essential operations continue during and after disruptive events. Grounded in the ISO 22301(Business Continuity Management) family of standards, BCMS integrates incident response plans, proactive risk assessment, preparedness, and continual improvement processes into enterprise-wide management systems. The goal is to sustain critical functions while preserving stakeholder confidence and regulatory compliance.

This chapter explores the theoretical, managerial, and operational foundations of BCMS, situating them within global standards for *incident management* and *operational resilience*. Incident management establishes tactical mechanisms for identifying, responding to, and learning from disruptions. Operational resilience represents the strategic capability that enables organizations to adapt and maintain functionality in the face of uncertainty. Together, they create an integrated system of prevention, response, and recovery governed by the Plan–Do–Check–Act (PDCA) cycle—a continuous improvement model derived from quality management principles.



© 2025 York Partners (Publishing) LLC 

The three learning objectives are:

1. **Differentiate BCMS Components:** Readers will understand the relationships among business continuity strategy, management, and planning, as outlined in ISO 22301 and its companion standards (including ISO 22313, 22317, 22318, and 22331).
2. **Apply ISO Frameworks in Context:** Practical applications are demonstrated across sectors such as food production, healthcare, and manufacturing, highlighting compliance, resilience, and efficiency gains.
3. **Integrate Continuity with Enterprise Risk Management (ERM):** BCMS principles are aligned with COSO-based Enterprise Risk Management (ERM) and Supply Chain Continuity Management (SCCM), ensuring cohesive oversight and governance.

Ultimately, BCMS fosters organizational agility by institutionalizing resilience as a strategic capability. It transforms reactive responses into proactive governance, ensuring that every disruption becomes a catalyst for improvement.

# Introduction

Business Continuity Management Systems (BCMS) represent a structured, organization-wide approach to preventing, preparing for, responding to, and recovering from disruptive incidents. [1]. Within the broader discipline of *Supply Chain Management (SCM)*, BCMS plays an essential role in ensuring that organizations can sustain the continuity of material, information, and service flows during interruptions [2]. Because supply chains are inherently vulnerable to disruptions— from natural disasters to intentional attacks to supplier instability — BCMS provides the discipline that supports and extends traditional approaches to managing supply chain disruptions.

## Business Continuity Management Systems

Beyond its role in crisis preparedness, BCMS may also be understood as a process-improvement and management-efficiency system. Many organizations already perform informal continuity activities — workarounds, contingency plans, ad-hoc response


© 2025 York Partners (Publishing) LLC

procedures — but these efforts often arise from local experience or past incidents rather than from deliberate design. BCMS formalizes these "common knowledge" practices into a reliable, repeatable, and auditable management system that reduces variability and ensures that critical activities are consistently performed. Certification to standards such as the ISO 22301 (Business Continuity Management) family of standards reinforces this discipline by maintaining organizational focus, establishing periodic review cycles, and preventing continuity programs from drifting toward complacency [1]. Audits help organizations recalibrate what is "enough" preparedness, ensuring resources are used effectively without overbuilding unnecessary response measures.

A core value of BCMS is that it provides a specific perspective on the business, focusing attention on the functions, dependencies, and vulnerabilities that matter most to sustaining operations. Rather than viewing resilience as a narrow technical task, BCMS reframes continuity as a cross-functional, enterprise-wide management viewpoint — a lens through which leadership evaluates strategy, governance, and risk. This perspective is dynamic: as business risks evolve, continuity strategies, recovery priorities, and preparedness practices must evolve as well. BCMS is therefore a continuous improvement discipline, not a static emergency plan. Through the Plan–Do–Check–Act (PDCA) model, organizations refine how they operate, adapting their processes to emerging threats, lessons learned, and advancements in technology or supply chain structure [3, 4].

## Literature Review

A literature review was conducted on the topic of business continuity management system and the foundation based on ISO 22301 "Security and resilience — Business continuity management systems — Requirements" [1].

The *methods* used for this scholarly literature search began with selecting the Scopus scholarly, scientific, and peer-reviewed article database. [5]. To maintain a consistently high standard of peer-reviewed content, the search was limited to journal articles and


© 2025 York Partners (Publishing) LLC

excluded books, book chapters, reports, and conference proceedings. Scopus was queried using the key terms “business continuity management systems” and “ISO 22301.”

The initial *results* returned to a surprisingly low 107 articles, including fifty-nine for the BCMS term alone. Only English-language publications were included, with translated versions added if the original article was officially published in multiple languages. Publications appeared across several disciplines, including thirty-one in Computer Science, thirty in Engineering, twenty-seven in Business/Management and Accounting, eleven in Decision Sciences, and ten in Economics/Econometrics and Finance.

Because ISO 22301 was first published relatively recently in 2012, and to focus on the most current applications, the search period was restricted to the last ten years (2016 to 2026). During that period, Scopus included eighty-one relevant documents (thirty-eight articles, thirty-one conference papers, eight book chapters, and three books). To ensure business-focused insights, the final inclusion criteria were restricted to peer-reviewed journal articles in the Business and Economics disciplines published since 2016.

The final set of documents consisted of fourteen articles. Full-text PDFs were retrieved and used as the primary library for the literature review. ChatGPT was used—cited in accordance with APA 7th edition [6, 7] — to generate initial summaries, after which the author validated and refined the insights by reviewing the original articles. Several preliminary verification steps were conducted to ensure ChatGPT could reliably read and interpret content from various document formats, including tests using Excel exports, Word files, and different PDF structures. Additional validation included querying specific text passages and confirming the correct document source identification.

Across the fourteen articles, Business Continuity Management Systems (BCMS) and ISO 22301 appear as either core organizing principles or supporting continuity constructs. Several studies directly formalize BCMS adoption. Suresh et al. develop a supply-chain continuity framework explicitly structured around ISO 22301 and its PDCA cycle [8]. Chen’s longitudinal case of Huawei demonstrates how ISO 22301 certification accelerated BCM maturity, integrated risk management, and improved operational resilience [9]. Loyarte et


© 2025 York Partners (Publishing) LLC

al. propose *Continuity Governance* as a new ISO-aligned process stage to enhance resilience within certified organizations [10].

Quantitative and optimization-driven studies assume BCMS as foundational. Rezaei Soufi et al. design mathematical models for selecting continuity plans based on BCMS requirements, including Recovery Time Objective (RTO, how fast to get back online) and Recovery Point Objective (RPO, how much data loss is acceptable) constraints embedded in ISO 22301 logic [11]. Paunescu's two works on SME preparedness [12] and risk-based recovery controls [13] use recovery metrics standard to BCMS, though not always tied explicitly to ISO.

Several articles treat BCMS more conceptually. Hassel et al. examine multi-actor crisis coordination, where BCM structures inform interorganizational preparedness, but ISO 22301 is not central to this study [14]. Loyear discusses tactical controls for unpredictable events, referencing continuity principles rather than formal BCMS adoption [15]. Russo et al. introduce a self-assessment approach for business continuity readiness rather than ISO-defined BCMS stages [16]. Buzzo & Rizzi ground resilience in dynamic capabilities, positioning BC as an outcome rather than as an ISO-driven system [17].

Sector-specific analyses — supply-chain disruptions [8], COVID-19 impacts [9], ICT and agricultural system continuity [13, 18], and continuity of critical functions [12] — use BC metrics (RTO, availability, redundancy), even when not tied to ISO.

Overall, BCMS/ISO 22301 is central in the framework, governance, and quantitative methods in four articles ([8-10, 14]), and tangential in resilience-oriented or sector-specific works in the remaining ten articles ([9, 10, 14, 19, 20]).


© 2025 York Partners (Publishing) LLC 

# BACKGROUND

## Positioning BCMS Within Enterprise Risk Management

BCMS does not exist in isolation. It interacts with and depends upon several interrelated management disciplines, including Quality Management Systems (QMS), Risk Management, and Enterprise Risk Management (ERM) structures, such as within the COSO framework [1, 3, 4, 21]. To clarify these relationships, the four-circle Venn-style conceptual diagram depicting the interconnections among: COSO-Based Enterprise Risk Management, Quality Management and traditional risk management functions, Business Continuity Management Systems, and Standards and Certifications (such as ISO 22301) (**Figure 1**).


***Figure 1 Interaction Business Management of Incident Management, Operational Resilience, Business Continuity Management, and the overall coordinating Enterprise Risk Management (ERM) System***

Figure 1 Illustrates that BCMS draws simultaneously from strategic risk governance, operational quality mechanisms, and validated international standards-based frameworks. The overlapping regions highlight how resilience emerges not from any single


© 2025 York Partners (Publishing) LLC

discipline but from the integration of all four domains. The most effective positioning is where the four systems intersect (identified by the triangle in the figure). For example:

- *COSO ERM* defines strategic alignment, governance, and risk appetite.
- *Quality and risk management* provide operational controls and a defect-prevention mindset.
- *Business Continuity Management System (BCMS)* applies structured continuity and recovery methodologies.
- *Standards and certifications* based on food safety management system standards) provide formalized requirements and benchmarking (e.g., ISO 22301, ISO 22313, Global Food Safety Initiative GFSI) [1, 22-27].

The diagram, therefore, reinforces a central message of this chapter: BCMS is most effective when positioned as part of an integrated management system, supported by the organization's governing frameworks, operational processes, and assurance mechanisms.

## Overview of ISO TC 292 and the ISO 22301 Family

International Standard Organization (ISO) Technical Committee (TC) 292 (ISO TC 292) focuses on security and resilience, producing globally recognized frameworks that help organizations manage risks and sustain operations [28]. The ISO 22301 standard specifies the requirements for a BCMS, while companion documents— ISO 22301 (Business Continuity Management), ISO 22313 (Guidance), ISO 22317 (Business Impact Analysis), ISO 22318 (Supply Chain Continuity), ISO 22316 (Principles and attributes), and ISO 22331 (Business Continuity Strategy)—provide detailed guidance on implementation and specialization. **Table 1** summarizes the purpose of each standard [1, 22, 29-32].

Adoption of these standards yields several strategic benefits: it demonstrates compliance with international best practice, enhances credibility with regulators and partners, and improves decision-making during crises. Within supply-chain environments, the ISO 22301 family ensures that continuity considerations extend to suppliers, logistics providers, and


© 2025 York Partners (Publishing) LLC

customers—creating an ecosystem of resilience rather than isolated silos of preparedness.

***Table 1 The Role and Key Differences of Each Business Continuity-Related ISO Standard [1, 22, 29-31]***

| ISO Standard | Primary Focus | Type of Document | Scope of Application | BCMS Integrated Activities |
|---|---|---|---|---|
| ISO 22301 | Defines BCMS requirements for certification | Requirements Standard | Broad, all sectors | Framework for implementing and auditing a BCMS |
| ISO 22313 | Explain how to apply ISO 22301 | Guidance Document | Implementation-specific | Practical interpretation and examples |
| ISO 22317 | Conducting Business Impact Analysis (BIA) | Guidance Document | Functional | Identifies critical processes and recovery priorities |
| ISO 22318 | Managing Supply Chain Continuity | Guidance Document | Sector-specific | Addresses vulnerabilities in external dependencies |
| ISO 22331 | Developing Continuity Strategies | Guidance Document | Strategic | Aligns strategies with organizational goals |

## Introduction to the Key Foundational Principles of Business Continuity Management

The ISO 22301 Business Continuity Management Systems (BCMS) family of standards provides the structural requirements and guidance for a Business Continuity Management System (BCMS), but understanding continuity in practice requires clarity on three foundational components: Business Continuity Strategy (BCS), Business Continuity Management (BCM), and Business Continuity Planning (BCP) [1]. These elements work together to form a coherent system of governance, preparedness, and operational response.


© 2025 York Partners (Publishing) LLC

From a supply-chain perspective, these components frame how organizations anticipate, prevent, and respond to disruptions. BCMS functions not only as a resilience framework but also as a process-improvement and management-efficiency system, integrating practices that many organizations already perform informally. Activities such as incident response, supplier backup arrangements, or IT recovery procedures often arise organically from past experience; BCMS provides the structure, documentation, and reliability needed to elevate them into formal, repeatable processes. Certification and audits further help organizations maintain focus, recalibrate the level of preparedness necessary, and avoid both under- and over-investment.

At a conceptual level, BCMS offers a specific lens through which the organization examines its operations, highlighting critical functions, dependencies, vulnerabilities, and acceptable downtimes. This perspective is not static. As risks, technologies, business models, and supply chains evolve, continuity processes must evolve as well. Thus, BCMS represents a continuous, dynamic cycle of refinement, consistent with the Plan–Do–Check–Act (PDCA) model described earlier.

To introduce the foundational elements of continuity, the following sections differentiate Strategy, Management, and Planning, while **Table 2** provides a comparative view of their scope, purpose, formality, and examples. This section draws on standards and scholarly resources [1, 3-35].

**1. Business Continuity Strategy**

A Business Continuity Strategy defines the organization's high-level approach to sustaining critical operations during and after a disruption. It articulates the "what" and "how" of continuity—recovery priorities, acceptable downtime thresholds, resource needs, and preferred methods of maintaining operations. Strategy decisions form the basis for all subsequent continuity planning.


© 2025 York Partners (Publishing) LLC

- **Business Continuity Strategy (BCS) Definition:** High-level organizational approach for maintaining essential functions during disruptions.
- **Focus:** Prioritization of operations, resource allocation, and options such as alternate sites or redundant capabilities.
- **Purpose:** Establishes the foundation for BCMS decision-making and response.
- **Formality:** Documented within the BCMS and aligned with organizational objectives.
- **Example:** Selecting an alternate operating location if the primary facility becomes unusable.

**2. Business Continuity Management (BCM)**

Business Continuity Management is the holistic management system that governs how continuity is implemented and maintained. BCM integrates strategy, policy, roles and responsibilities, exercises, and improvement processes to ensure that resilience becomes an organizational capability rather than a collection of isolated activities.

- **Business Continuity Management (BCM) Definition:** A management framework for identifying threats, assessing impacts, and ensuring continuity across the enterprise.
- **Focus:** Enterprise governance, oversight, integration with risk management, and continual improvement.
- **Purpose:** Provides structure and accountability for resilience activities.
- **Formality:** A fully formalized system embedded within overall risk governance.
- **Example:** Establishing a BCM office with defined roles and periodic plan testing.

**3. Business Continuity Planning (BCP)**

While BCM provides the governance system, Business Continuity Planning creates the detailed, operational procedures used to respond to and recover from disruptions. BCP translates strategy into step-by-step processes and documentation.


© 2025 York Partners (Publishing) LLC

- **Business Continuity Planning (BCP) Definition:** Operational plans describing how to restore critical activities after an incident.
- **Focus:** Recovery procedures, communication protocols, IT restoration, and process-specific instructions.
- **Purpose:** Ensures that personnel can act quickly and effectively to reduce downtime.
- **Formality:** Highly formalized, documented, and tested; includes BIA outputs (MTD, RTO) and Disaster Recovery Plans (DRPs).
- **Example:** A communications plan for notifying stakeholders during an outage.

**Relationship Among BCS, BCM, and BCP**

Together, these components form a hierarchical and interdependent system:

- **BCS (Strategy)** establishes direction.
- **BCM (Management)** provides the governance and structure to implement that direction.
- **BCP (Planning)** delivers the operational capability to execute it.

This table summarizes their differences in scope, purpose, formality, and illustrative examples. This table is an essential reference for readers who are new to continuity concepts, as it clarifies how each component contributes to an integrated resilience program.


© 2025 York Partners (Publishing) LLC

***Table 2 Comparison of Business Impact Analysis (ISO 22317) and Supply Chain Continuity (ISO 22318) [30, 31]***

| Aspect | Business Continuity Strategy | Business Continuity Management | Business Continuity Planning |
|---|---|---|---|
| **Scope** | Focused on high-level approaches and goals. | Encompasses strategy, planning, governance, and testing. | Detailed, step-by-step operational response plans. |
| **Purpose** | Defines "what" and "why" for continuity. | Provides a holistic framework for resilience. | Provides the "how-to" for specific disruptions. |
| **Formality** | Documented as part of BCM. | Formalized governance process. | Highly formalized, detailed, and operational. |
| **Example** | Identifying alternative suppliers. | Establishing a BCM office with oversight roles. | Creating an IT recovery plan for outages. |

## Principles of Business Continuity Management

Business continuity management is underpinned by several interrelated *principles* derived from organizational resilience theory, quality management, and enterprise risk management. These *principles* provide both philosophical and operational grounding for an effective BCMS. This section draws on standards and scholarly resources [34, 36-38].

### 1. Integration and Alignment

Business continuity management processes must be integrated with corporate governance, strategic planning, and risk management systems. When business continuity is aligned with enterprise risk management (ERM) and COSO frameworks, the organization achieves consistency between its tolerance for risk and its preparedness for disruption. Integration ensures that continuity measures are not peripheral activities but embedded within core business processes.

### 2. Leadership Commitment

Top management plays a decisive role in establishing a business continuity culture. Leadership defines risk appetite, allocates resources, and approves recovery strategies. The board of directors maintains ultimate accountability for ensuring that the organization possesses competent, documented systems capable of sustaining operations under


© 2025 York Partners (Publishing) LLC

stress. ISO 22301 requires that leadership demonstrate commitment through policy, objectives, and ongoing review.

### 3. Risk-Based Thinking

BCMS operates on a proactive, risk-based mindset. Organizations identify threats and vulnerabilities, evaluate potential impacts through Business Impact Analysis (BIA), and prioritize recovery objectives such as maximum tolerable downtime (MTD) and recovery time objectives (RTO). This structured assessment forms the basis for selecting continuity strategies proportionate to the organization's risk exposure.

### 4. Continual Improvement

Resilience is a dynamic capability. The PDCA cycle mandates routine evaluation, testing, and refinement of continuity plans. Lessons learned from incidents, exercises, and audits feed back into updated procedures. Through this iterative process, resilience maturity increases, leading to improved efficiency and reduced recovery times.

### 5. Stakeholder Engagement

Effective continuity management recognizes that disruptions affect multiple stakeholders—employees, customers, suppliers, regulators, and communities. Transparent communication and coordinated collaboration are essential. Stakeholder mapping and engagement plans help ensure that expectations are managed and trust is maintained throughout a crisis.

.

*The next section, Foundational Scholarly Business Strategy Theories, expands these principles by connecting BCMS to academic frameworks such as contingency theory, high-reliability organization theory, and dynamic capabilities. These models explain why certain organizations achieve resilience, and others falter under comparable conditions.*


© 2025 York Partners (Publishing) LLC

## Theories of Business Continuity Management

Business continuity strategy synthesizes management science, organizational theory, and risk governance. Scholarly frameworks illuminate how resilience becomes an enduring capability rather than a one-time project. The *theories* summarized below anchor BCMS within established management research and provide a vocabulary for continuous improvement.

### 1. Business Continuity Management (BCM) Framework

The BCM framework defines a structured cycle for identifying potential threats, assessing their impacts, and developing coordinated responses. It includes risk assessment, business-impact analysis (BIA), strategy formulation, plan development, testing, and maintenance. Scholars emphasize embedding BCM within enterprise risk management to ensure that continuity objectives complement corporate goals rather than compete with them.

### 2. Resilience Engineering

Resilience engineering views organizations as adaptive systems capable of anticipating, absorbing, and recovering from stress. Four qualities characterize resilient systems:

- **Flexibility:** the ability to adjust to changing conditions.
- **Redundancy:** backup capacity to maintain operations when components fail.
- **Resourcefulness:** rapid identification of problems and mobilization of solutions.
- **Rapidity:** speed of detection, response, and recovery.

These qualities align directly with the PDCA cycle and the ISO 22301 requirement for continual improvement.


© 2025 York Partners (Publishing) LLC

### 3. High-Reliability Organization (HRO) Theory

HRO theory examines entities that operate in complex, high-risk environments yet maintain exceptional safety and reliability—such as aviation or nuclear power. Its principles apply equally to BCMS:

1. **Preoccupation with Failure:** continuous vigilance for weak signals of risk.
2. **Reluctance to Simplify:** careful analysis of system complexity.
3. **Sensitivity to Operations:** awareness of frontline realities.
4. **Commitment to Resilience:** capacity to absorb errors and adapt.
5. **Deference to Expertise:** valuing operational knowledge over hierarchy.

Integrating HRO practices into continuity management helps organizations avoid "normalization of deviance," where small anomalies are ignored until they cascade into crises.

### 4. Contingency Theory

Contingency theory asserts that management effectiveness depends on contextual fit; there is no universal model for resilience. BCMS strategies must therefore be tailored to each organization's size, industry, and environment. Large global supply chains require formal governance and documentation, while smaller firms benefit from agility and simplified procedures. This contextualization explains the adaptability of the ISO 22301 framework across sectors.

### 5. Stakeholder Theory

Stakeholder theory expands continuity planning beyond internal processes to consider all affected parties. During disruptions, maintaining communication with employees, customers, regulators, and communities preserves legitimacy and trust. Proactive engagement transforms crisis response into an opportunity for relationship strengthening, reinforcing long-term resilience.


© 2025 York Partners (Publishing) LLC

### 6. Dynamic Capabilities Framework

Dynamic capabilities describe an organization's ability to sense, seize, and transform resources in response to change. Within BCMS, sensing equates to early detection of emerging risks, seizing involves implementing continuity strategies, and transforming entails institutional learning after an incident. This framework operationalizes the notion of continual improvement and directly supports the PDCA methodology.

### 7. Crisis Management Models

Crisis management provides a tactical complement to strategic continuity. Common models delineate three phases: **pre-crisis** (prevention and preparedness), **crisis response** (immediate containment and communication), and **post-crisis** (recovery and learning). Integrating these phases into BCMS ensures that incident management is both reactive and generative—each event yields insights into future prevention.

### 8. Enterprise Risk Management (ERM)

Enterprise Risk Management, as defined by COSO, offers a holistic framework for identifying, assessing, and mitigating risks across the enterprise. Embedding BCMS within ERM ensures that continuity planning is governed by the same risk appetite and reporting mechanisms that guide strategic decision-making. ERM integration also satisfies regulatory expectations for oversight under statutes such as the U.S. Sarbanes-Oxley Act (SARBOX). While ERM was first created to meet the US regulatory requirements of SARBOX, the underlying principles were already implemented in most companies and are also common requirements for global regulations. For example, the European Union has the Audit Directive (2006/43/EC) and Transparency Directive (2004/109/EC), China has its own SOX-type framework in the Enterprise Internal Control Standard, and also other regions, including other countries such as Canada (C-SOX) and Japan (J-SOX). The ERM-type basic principles and theories are universal.


© 2025 York Partners (Publishing) LLC

### 9. Operational Resilience (OR)

Operational resilience represents the outcome of mature continuity and incident-management systems. ISO 22316 defines resilience as the ability to continue delivering critical operations under disruption ([32] also see [39]). In practice, operational resilience depends on data from incident management systems (IMS) and on board-level governance that enforces accountability for risk tolerance and recovery performance.

.

*Collectively, these theories affirm that resilience is not a static state, but a continual capability rooted in governance, culture, and learning. By drawing on BCM, HRO, contingency, and dynamic-capability frameworks, organizations build BCMS programs that are both systematic and adaptive*.

# Business Continuity Compliance and Enterprise Risk Management (ERM)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a widely adopted framework for Enterprise Risk Management (ERM) [21, 40, 41]. Within this framework, business continuity is not an isolated activity; it forms a core element of risk governance and strategic performance. Embedding BCMS into COSO ERM ensures that continuity planning, testing, and oversight are treated as continuous control processes rather than emergency measures. This section draws upon several primary sources [40-44].

### 1. Strategic Integration

BCMS must align with the organization's mission, vision, and strategic objectives. COSO ERM requires linking risk appetite and risk tolerance to performance measures, so that continuity priorities support—not compete with—long-term goals. This integration ensures


© 2025 York Partners (Publishing) LLC

that resources devoted to continuity strengthen overall competitiveness and stakeholder confidence.

**2. Risk Identification and Assessment**

Organizations identify risks that could interrupt critical functions—natural disasters, cyberattacks, supply-chain failures, or pandemics. Scenario analysis and stress testing, consistent with COSO principles, quantify potential impacts on strategic, operational, and compliance objectives. Outputs from Business Impact Analysis (BIA) inform ERM risk registers and dashboards.

**3. Business Impact Analysis (BIA)**

A BIA evaluates the effect of disruptions on operations, finances, and reputation. It defines recovery priorities, maximum tolerable downtime (MTD), and recovery time objectives (RTO). COSO ERM emphasizes documentation of these metrics as control activities subject to periodic review.

**4. Risk Responses and Controls**

Continuity controls — preventive, detective, and corrective — are developed to mitigate identified risks. Examples include redundant data centers, cross-training of key personnel, and alternate supply routes. Controls are monitored through internal audits and management reviews, fulfilling COSO's internal-control component.

**5. Embedding Resilience and Flexibility**

COSO ERM stresses embedding resilience into organizational culture. Redundancy, adaptability, and flexibility are designed into systems and processes. Training, simulations, and tabletop exercises reinforce competence at all levels, converting theoretical plans into practiced behaviors.


© 2025 York Partners (Publishing) LLC

## 6. Integration with Crisis Management

Crisis-management planning complements continuity by establishing roles, communication protocols, and escalation procedures. During an incident, the Crisis Management Team (CMT) coordinates tactical response while BCMS maintains strategic oversight. The linkage ensures both rapid containment and sustained governance.

## 7. Monitoring and Reporting

Continuous monitoring provides assurance that continuity measures remain effective. Key Performance Indicators (KPIs) include test completion rates, recovery times, and post-incident corrective-action closure. Reports to senior management and the board demonstrate compliance with regulatory and fiduciary obligations.

## 8. Regulatory Compliance and Governance

By aligning BCMS with COSO ERM, organizations satisfy external regulations such as the Sarbanes-Oxley Act (US) or the UK Corporate Governance Code. Governance structures assign accountability to senior management and board-level committees, integrating continuity into overall assurance frameworks.

## 9. Technology and Data Resilience

COSO emphasizes safeguarding information assets. Disaster-recovery plans (DRPs), cybersecurity controls, and secure data-backup regimes are continuity components that directly support IT governance and privacy compliance.

## 10. Testing, Training, and Continuous Improvement

Regular testing validates plan feasibility; training ensures readiness. Results feed into the PDCA cycle, closing the loop between ERM oversight and operational execution. Each test is an opportunity to refine both continuity procedures and risk appetite assumptions.


© 2025 York Partners (Publishing) LLC

.

*Integrating BCMS into COSO ERM transforms continuity from a reactive safeguard into a proactive governance discipline. The outcome is a resilient organization where strategic intent, operational capacity, and stakeholder expectations remain aligned under stress.*

# International Standards Organization (ISO) Guidance and the ISO 22301 Family of Standards

The International Standards Organization (ISO) is a global body that develops frameworks promoting safety, quality, and resilience. Its Technical Committee 292 (ISO/TC 292) produces the security and resilience standards, including the 22301 series that forms the foundation of Business Continuity Management Systems (BCMS) [28, 45]. These standards provide a common language and structure across industries and geographies, helping organizations manage disruptions systematically.

## ISO TC 292 Scope and Purpose

ISO/TC 292's mandate is to enhance organizational and societal resilience by establishing uniform practices for risk management, emergency response, and continuity planning. Participation includes experts from government, academia, and the private sector, ensuring that standards are both globally applicable and practical. The committee's publications enable interoperability among national regulations and industry frameworks, reducing redundancy and confusion in continuity planning.

### 1. ISO 22301 – Business Continuity Management Systems: Requirements

**ISO 22301** is the primary requirements standard for establishing, implementing, maintaining, and continually improving a BCMS [1]. It outlines governance, policy, leadership, operational planning, support, and performance evaluation. The standard applies to organizations of all sizes and sectors and emphasizes:


© 2025 York Partners (Publishing) LLC

- **Context and Leadership:** Defining internal and external issues, stakeholders, and leadership commitment.
- **Planning:** Establishing objectives, risk assessments, and business-impact analyses (BIAs).
- **Operation:** Implementing continuity strategies and response structures.
- **Performance Evaluation:** Monitoring, measurement, analysis, and management review.
- **Improvement:** Continual refinement via corrective actions and audits.

ISO 22301 ensures that continuity planning is proactive, evidence-based, and auditable, turning resilience into a management function rather than an ad-hoc response.

### 2. Supporting Standards in the ISO 22301 Family

The ISO 22301 family includes several complementary guidance documents. Together, these standards create a comprehensive architecture for continuity management (Table 3).

- **ISO 22313 – Guidance for Implementation:** Provides interpretive guidance and examples for applying the ISO 22301 requirements [22].
- **ISO 22317 – Guidelines for Business Impact Analysis:** Outlines methodology for assessing the effects of interruptions on critical functions [31].
- **ISO 22318 – Guidelines for Supply Chain Continuity:** Focuses on identifying vulnerabilities and developing strategies to ensure the flow of goods and services [30].
- **ISO 22331 – Guidelines for Business Continuity Strategy:** Guides development of strategies tailored to an organization's risk profile and resource constraints [29].


© 2025 York Partners (Publishing) LLC

***Table 3 Overview of the key differences among the ISO 22301, 22313, 22317, 22318, and 22331 standards [1, 22, 29-31]***

| ISO Standard | Primary Focus | Type of Document | Scope | Level of Detail | Practical Application |
|---|---|---|---|---|---|
| **ISO 22301** | Requirements for a BCMS | Standard specifying requirements | Broad and applicable to all sectors | High-level requirements | Provides a framework to establish, implement, and maintain a BCMS. |
| **ISO 22313** | Guidance for implementing ISO 22301 | Guidance document | Implementation-specific | Detailed guidance | Offers practical advice on applying ISO 22301 requirements. |
| **ISO 22317** | Business Impact Analysis (BIA) | Guidance document | Focused on BIA processes | Detailed analysis methodologies | Help organizations identify critical activities and assess disruption impacts. |
| **ISO 22318** | Supply Chain Continuity | Guidance document | Supply chain-specific | Sector-specific guidance | Focuses on supply chain vulnerabilities and continuity strategies. |
| **ISO 22331** | Business Continuity Strategy | Guidance document | Strategic level | Strategic guidance | Aids in selecting and implementing continuity strategies tailored to risks and goals. |

### 3. Complementary Roles of ISO 22317 and ISO 22318

ISO 22317 and ISO 22318 expand the ISO 22301 framework by addressing two complementary dimensions of continuity: internal business-impact assessment and external supply-chain resilience. ISO 22317 identifies critical activities and recovery priorities, while ISO 22318 builds upon those insights to protect supply-chain dependencies through risk mitigation and supplier collaboration. Together, they provide an integrated view of continuity across organizational and network vulnerabilities.

**ISO 22301 and ISO 22313** form the foundation; certification is based on ISO 22301.

- **ISO 22317, 22318, and 22331** extend into analysis, supply-chain resilience, and strategic alignment.
- The family of standards reflects the maturity of global continuity practices—moving from reactive recovery to proactive resilience.


© 2025 York Partners (Publishing) LLC

## Benefits of ISO Adoption

1. **Global Consistency:** Ensures common terminology and alignment across supply chains.
2. **Compliance and Credibility:** Demonstrates due diligence to regulators, insurers, and customers.
3. **Efficiency:** Streamlines internal processes and eliminates duplication among risk, quality, and safety systems.
4. **Learning and Improvement:** The PDCA model embedded in ISO 22301 institutionalizes feedback and innovation.

ISO's contribution to business continuity lies in translating abstract resilience concepts into structured, auditable requirements. The 22301 family gives organizations a common framework to plan, implement, test, and improve their continuity programs—creating a globally interoperable language of resilience.

# Supply Chain Continuity Management (SCCM)

Supply Chain Continuity Management (SCCM) extends the principles of business continuity to encompass the entire network of suppliers, logistics providers, distributors, and customers [30]. Given that modern organizations operate within complex global supply chains, disruptions at any point in the network can cascade into significant operational, financial, and reputational impacts. SCCM ensures resilience beyond the boundaries of the organization by managing dependencies and sustaining material, information, and service flows under adverse conditions.


© 2025 York Partners (Publishing) LLC

## Supply Chain Continuity Management (SCCM)

The goal of SCCM is to prevent, prepare for, and respond to supply chain disruptions in a way that maintains continuity of critical goods and services. SCCM aligns with ISO 22318 (Guidelines for Supply Chain Continuity) and supports ISO 22301's system-level approach to resilience. It incorporates assessment of supplier reliability, logistics redundancy, and end-to-end risk visibility.

There are several key elements of SCCM:

1. **Supply Chain Risk Identification**

Organizations map their supply networks to identify single points of failure, such as sole-source suppliers or constrained logistics hubs. Tools like Failure Mode and Effects Analysis (FMEA) and supply chain mapping software are used to visualize dependencies and vulnerabilities.

2. **Business Impact Analysis for Supply Chains**

BIA in SCCM evaluates the effects of supplier disruptions on business operations. It identifies critical inputs, assigns recovery priorities, and quantifies the operational and financial impacts of supply interruptions.

3. **Risk Mitigation and Strategy Development**

Continuity strategies include diversification of suppliers, establishing alternate logistics routes, maintaining safety stock, and developing mutual-aid agreements. ISO 22318 emphasizes collaboration with suppliers to ensure mutual resilience and continuity obligations.


© 2025 York Partners (Publishing) LLC

4. **Testing and Validation**

Regular supplier audits, continuity tests, and joint exercises validate the resilience of the supply chain. These tests ensure that business continuity plans (BCPs) are practical, coordinated, and aligned across the value chain.

5. **Communication and Collaboration**

Transparent communication with suppliers and customers strengthens trust during crises. Shared dashboards and early-warning systems provide visibility into inventory, transport, and production statuses.

## Sector Examples: Practical Examples of Supply Chain Continuity Management (SCCM)

Supply Chain Continuity Management (SCCM) is critical in industries where even brief disruptions can produce cascading operational, financial, and regulatory consequences. The following examples illustrate how SCCM principles — particularly those reflected in ISO 22318 — are applied to strengthen resilience in diverse sectors. Each scenario highlights the need to understand vulnerabilities, build redundancy, implement early-warning mechanisms, and coordinate with key suppliers and partners.

1. **Food and Beverage Industry**

**Scenario:** A global food manufacturer relies on a single supplier for a high-risk, high-value ingredient such as cocoa, dairy proteins, or fermentation cultures.

**Expanded SCCM Applications**

- **Supplier diversification:** To avoid dependence on one region or climate-sensitive crop, the company establishes multi-regional supplier agreements and develops a tiered supplier strategy based on risk exposure.
- **Inventory and safety-stock strategy:** Time-phased buffers are created for critical ingredients, adjusted seasonally, and linked to demand forecasts and shelf-life constraints.


© 2025 York Partners (Publishing) LLC

- **Integrated supplier audits:** Audits now include **continuity-specific criteria** such as backup production lines, crisis communication capabilities, and energy resilience.
- **Logistics and transportation contingency planning:** Alternate shipping lanes, modal substitutions (sea to air), and pre-approved customs brokers ensure product flow even during geopolitical or infrastructure-related disruptions.
- **Alignment with food safety systems:** Continuity strategies are cross-checked against Food Safety Management System (FSMS) requirements (e.g., HACCP, Global Food Safety Initiative – GFIS, and ISO 22000) to prevent substitution or re-routing from introducing food safety risks.

The ISO 22301 family not only establishes the foundation for Business Continuity Management Systems but also provides specialized guidance that supports continuity across sector-specific frameworks, including Food Safety Management Systems (FSMS) based on ISO 22000 (Food Safety Management) [46]. The following table summarizes key standards within the ISO 22301 series and illustrates how each contributes to food safety management and resilience in food production and supply-chain operations. By clarifying scope, purpose, and application (Table 4). shows how these standards reinforce the continuity components essential to maintaining food safety, regulatory compliance, and operational reliability. Together, they create an integrated framework that links business continuity principles with the unique requirements and controls embedded within FSMS.

***Table 4 ISO Standards for Business Continuity and the Food and Beverage Industry, topic of Food Safety Management [1, 22, 29-31]***

| ISO Standard | Title | Scope Summary (25 words) | Application for Food Safety Management (25 words) |
|---|---|---|---|
| ISO 22301 | Business Continuity Management Systems -- Requirements | Defines requirements for implementing, maintaining, and improving a BCMS to ensure organizational resilience and recovery from disruptions. | Help food companies ensure resilience against disruptions, safeguarding operations, and compliance with food safety standards. |


© 2025 York Partners (Publishing) LLC

| | | | |
|---|---|---|---|
| ISO 22313 | Business Continuity Management Systems -- Guidance | Provides guidance for implementing ISO 22301, including examples and interpretations to support BCMS effectiveness and integration. | Supports food safety managers in embedding continuity planning into food production and supply processes. |
| ISO 22317 | Guidelines for Business Impact Analysis (BIA) | Offers methodologies to identify critical functions, assess disruption impacts, and set recovery priorities through Business Impact Analysis (BIA). | Enables food producers to identify critical processes, evaluate risks to safety compliance, and prioritize recovery efforts. |
| ISO 22318 | Guidelines for Supply Chain Continuity | Focuses on identifying supply chain vulnerabilities, assessing risks, and developing strategies to ensure continuity of goods and services. | Ensures the continuity of food supply chains, safeguarding critical ingredients, logistics, and supplier reliability. |
| ISO 22331 | Guidelines for Business Continuity Strategy | Guides to the development of continuity strategies aligned with risks, resources, and organizational goals to ensure effective disruption responses. | Supports the alignment of food safety strategies with continuity planning to protect against disruptions in production or distribution. |

### 2. Pharmaceutical Industry

**Scenario:** A pharmaceutical company depends on active pharmaceutical ingredient (API) suppliers located in regions with geopolitical instability.

**Expanded SCCM Applications**

- **Risk and vulnerability assessment:** The company conducts structured risk analyses that include country risk ratings, regulatory constraints, transportation reliability, and laboratory capacity for quality verification.
- **Redundant and qualified suppliers:** Secondary suppliers undergo full GMP and regulatory qualification to ensure rapid activation without delays in US Food and Drug Administration (FDA) or EMA approval.
- **Regulatory continuity management:** Change-control procedures are pre-documented so alternate suppliers can be activated with minimal regulatory disruption.
- **Supplier alignment and testing:** Joint emergency drills simulate API production outages, testing communication pathways, quality release procedures, and logistics rerouting.


© 2025 York Partners (Publishing) LLC

- **Cold chain and controlled-environment continuity:** Temperature-controlled storage and transport redundancies are built to prevent spoilage and non-compliance during disruptions.

### 3. Automotive Industry

**Scenario:** An automaker faces severe semiconductor shortages, threatening just-in-time (JIT) assembly operations.

**Expanded SCCM Applications**

- **End-to-end supply chain mapping:** Detailed mapping extends beyond Tier 1 suppliers to Tier 2 and Tier 3 silicon foundries, raw wafer producers, and packaging facilities.
- **Early-warning and predictive analytics:** Tools monitor capacity utilization, lead times, and geopolitical developments affecting semiconductor manufacturing hubs.
- **Joint continuity planning:** Automakers collaborate closely with chipmakers to share forecast data and co-create continuity plans, including guaranteed minimum allocations.
- **Localization and nearshoring:** Production shifts toward regional semiconductor plants or modular designs that allow component substitution.
- **Design-for-resilience:** Engineering teams redesign vehicle systems to reduce dependence on scarce or single-source chips.

### 4. Retail Sector

**Scenario:** A global retail chain must secure holiday-season inventory while relying on congested international ports and long shipping lanes.

**Expanded SCCM Applications**

- **Advanced procurement and scheduling:** Orders are placed months earlier, with dynamic scheduling models that adjust shipping quantities based on demand trends and disruption signals.


© 2025 York Partners (Publishing) LLC

- **Alternative logistics routing:** Pre-negotiated contracts include bypass options for canal closures, port congestion, or regional labor strikes.
- **Supplier prioritization agreements:** Retailers negotiate surge arrangements that guarantee allocation of production capacity during peak seasons.
- **Digital visibility systems:** End-to-end tracking dashboards monitor vessel status, port queue times, and inland transport deviations to trigger contingency activation.

5. **Technology and Electronics Sector**

**Scenario:** A technology manufacturer confronts global component shortages affecting microchips, sensors, and power systems.

**Expanded SCCM Applications**

- **Strategic supplier partnerships:** Multi-year contracts include continuity clauses such as minimum inventory commitments and co-investment in production expansion.
- **Onshoring and nearshoring:** Critical components previously sourced globally are relocated closer to manufacturing plants, reducing geopolitical and logistics risk.
- **AI-enhanced demand forecasting:** Machine learning models predict fluctuations in consumer demand and component availability, enabling proactive procurement.
- **Supplier capability-building:** Companies invest in supplier training, cybersecurity enhancements, and BCM development to ensure alignment with ISO 22318 expectations.

6. **Healthcare Supply Chain**

**Scenario:** A hospital system must maintain an uninterrupted supply of medical-grade oxygen, pharmaceuticals, and personal protective equipment during a pandemic.

**Expanded SCCM Applications**

- **Regional diversification of suppliers:** Contracts include suppliers in different geographic regions to protect against localized manufacturing outages.


© 2025 York Partners (Publishing) LLC

- **Surge capacity modeling:** Hospitals collaborate with suppliers to plan for extreme peaks in demand, including pre-authorized production increases.
- **Strategic stockpile management:** Rotational inventory programs maintain readiness without compromising expiration dates or regulatory guidelines.
- **Critical delivery logistics:** Emergency transport methods such as airlift or specialized tank delivery routes are planned and periodically tested under simulated crisis conditions.
- **Integration with clinical operations:** Continuity plans are aligned with patient safety requirements, ensuring that shortages do not trigger hazardous substitutions or clinical delays.

**Common Strategies Across Industries**

Across all sectors, high-performing SCCM programs consistently apply several cross-cutting strategies:

1. **Supplier Collaboration:** Shared planning, transparency, and communication enhance mutual resilience.
2. **Redundancy:** Multiple suppliers, backup logistics routes, and safety stock reduce dependence on any one node.
3. **Supply Chain Visibility:** Digital tools and mapping systems expose vulnerabilities across tiers.
4. **Testing and Simulation:** Exercises validate supplier readiness and reveal operational gaps.
5. **Predictive and Digital Tools:** Data analytics, artificial intelligence (AI), and real-time monitoring improve decision-making and risk anticipation.

SCCM equips organizations to sustain operations, meet customer expectations, and support regulatory or safety obligations during disruptions. By applying ISO 22318 principles—supply chain vulnerability assessment, continuity strategy development, and supplier collaboration—organizations develop supply chains that are not only efficient but


© 2025 York Partners (Publishing) LLC

structurally resilient. These examples demonstrate how SCCM transforms continuity from reactive crisis response into proactive operational design.

**Integration with BCMS and ISO Frameworks**

SCCM acts as an operational layer of BCMS, translating high-level business continuity policies into actionable supply chain procedures. ISO 22318 directly links SCCM to ISO 22317 (Business Impact Analysis – BIA), ensuring that identified supply-chain risks feed into enterprise-level continuity strategies. When aligned with COSO ERM, SCCM provides cross-functional visibility into risk, enabling organizations to prioritize investment and resilience efforts based on quantitative impact analysis.

SCCM reinforces the notion that resilience is an ecosystem property. A single organization's continuity depends on its partners' stability, transparency, and adaptability. Implementing SCCM transforms supply chains from reactive networks into proactive, collaborative systems capable of sustaining operations amid uncertainty.

# Conclusion and Key Takeaways

## Conclusion

Business Continuity Management Systems (BCMS) provide a structured foundation for sustaining organizational performance and stakeholder confidence during disruption. Drawing upon the ISO 22301 family of standards, BCMS transforms continuity from an emergency response into an institutionalized management process governed by leadership, measured through performance metrics, and improved via the Plan–Do–Check–Act (PDCA) cycle.


© 2025 York Partners (Publishing) LLC

## Overview of BCMS

Throughout this chapter, we have shown that effective continuity management integrates incident management, operational resilience, and enterprise risk governance. Theoretical underpinnings—from resilience engineering and high-reliability organization theory to dynamic capabilities—illustrate that organizational resilience is not a fixed state but an evolving capability that thrives on learning and adaptation.

Compliance frameworks such as COSO's Enterprise Risk Management (ERM) embed continuity into corporate governance, ensuring accountability and regulatory alignment. Meanwhile, the ISO 22301 family provides a harmonized, auditable structure for designing, implementing, and improving continuity systems. Extending these principles across supply chains through ISO 22318 and Supply Chain Continuity Management (SCCM) ensures that resilience extends beyond individual organizations to encompass entire ecosystems.

In essence, BCMS represents the convergence of proactive strategy and operational discipline. By viewing resilience as a continuous process—anchored in governance, collaboration, and culture—organizations can anticipate change, recover rapidly, and emerge stronger after every disruption.

## Integrating BCM, Operational Resilience, and Incident Management within an Enterprise Risk – Aligned Value Chain

Business Continuity Management (BCM), operational resilience, and incident management are individually essential disciplines—each must operate efficiently on its own to ensure planning rigor, adaptive capacity, and rapid response. Yet their actual value emerges only when they are calibrated and interconnected within an organization's broader integrated supply chain management environment. In this integrated view, continuity planning safeguards critical processes, operational resilience enables systems and partners to absorb and adapt to shocks, and incident management orchestrates real-time actions across the value chain. Together, they support the organization's ability to remain viable, consistent, and competitive. Their collective performance is ultimately


© 2025 York Partners (Publishing) LLC

assessed through a COSO-based Enterprise Risk Management (ERM) lens, ensuring that risks are managed cohesively across functions and supply chain nodes. This manuscript is key to explaining the foundation and role of BCMS.

## Actionable Takeaways for Practitioners

1. **Institutionalize Integration**
   Embed BCMS within enterprise governance and risk management systems so that continuity data and lessons learned directly influence strategic decisions.
2. **Embed Accountability and Testing**
   Assign clear ownership for continuity performance at the board and executive levels. Conduct regular audits, simulations, and post-incident reviews to measure competence and preparedness.
3. **Promote Continuous Learning and Adaptation**
   Use every disruption or near miss as a case study for improvement. Apply the PDCA cycle rigorously to refine processes, enhance cross-functional communication, and advance resilience maturity.


© 2025 York Partners (Publishing) LLC

# REFERENCES


1. ISO, International Organization for Standardization, *ISO 22301, Security and resilience — Business continuity management systems — Requirements, [Accessed January 15, 2022], URL: https://www.iso.org/standard/75106.html*. 2019.
2. Spink, John, *Supply Chain Management Introduction: Sourcing, Operations & Logistics, ISBN 978-x-xx-xxxxxx-x*. IN PRESS.
3. ISO, International Organization for Standardization, *ISO 9000: 2015 Quality management systems -- Fundamentals and vocabulary, International Standards Organization (ISO), URL: https://www.iso.org/standard/45481.html*. 2015.
4. ISO, International Organization for Standardization, *ISO 31000:2018 Risk management -- Guidelines, URL: https://www.iso.org/standard/65694.html*. 2018.
5. Scopus. *Scopus Database, Elsevier. Retrieved December 7, 2025, from www.scopus.com*. 2025.
6. ChatGPT, *OpenAI. (2025). ChatGPT 5.0 (December 2025 version) [Large language model]. https://chat.openai.com/chat*. . 2025.
7. American Psychological Association, APA, *Publication manual of the American Psychological Association (7th ed.), www.APA.org*. 2020.
8. Suresh, N., G. L. Sanders, and M. J. Braunscheidel, *Business Continuity Management for Supply Chains Facing Catastrophic Events*. IEEE Engineering Management Review, 2020. **48**(3): p. 129-138.
9. Chen, S. and J. Xu, *COVID-19, business continuity management and standardization: case study of Huawei*. Chinese Management Studies, 2023. **17**(5): p. 1117-1138.
10. Loyarte, E., N. Gurrutxaga, and J. Funcia, *Continuity Governance model: a new process stage in the BCM system that underpins organizational resilience*. Cogent Business and Management, 2024. **11**(1).
11. Rezaei Soufi, H., S. A. Torabi, and N. Sahebjamnia, *Developing a novel quantitative framework for business continuity planning*. International Journal of Production Research, 2019. **57**(3): p. 779-800.
12. Păunescu, C., *How prepared are small and medium sized companies for business continuity management?* Quality - Access to Success, 2017. **18**(161): p. 43-48.
13. Păunescu, C., M. C. Popescu, and L. Blid, *Business impact analysis for business continuity: Evidence from Romanian enterprises on critical functions*. Management and Marketing, 2018. **13**(3): p. 1035-1050.
14. Hassel, H. and A. Cedergren, *A framework for business continuity management in a multiactor context*. Journal of Contingencies and Crisis Management, 2024. **32**(2).
15. Loyear, R., *Tactical security controls for unpredictable events: Aligning security tactics with business continuity for resilience in the face of the unknown*. Journal of Business Continuity and Emergency Planning, 2026. **19**(2): p. 102-118.
16. Russo, Nelson, Henrique São Mamede, and Leonilde Reis, *An approach to business continuity self-assessment*. Technologies, 2025. **13**(6): p. 242.
17. Buzzao, G. and F. Rizzi, *The role of dynamic capabilities for resilience in pursuing business continuity: an empirical study*. Total Quality Management and Business Excellence, 2023. **34**(11-12): p. 1353-1385.
18. Păunescu, C. and R. Argatu, *Critical functions in ensuring effective business continuity management. Evidence from romanian companies*. Journal of Business Economics and Management, 2020. **21**(2): p. 497-520.
19. Religia, A. A. and D. N. Utama, *A Novel Framework for Business Continuity Plan in Public Sector Organization*. Journal of System and Management Sciences, 2024. **14**(1): p. 1-14.
20. Andi, R. and D. N. Utama, *Business Continuity Management Framework In Electronic System Provider (ESP) Startup Company*. Journal of System and Management Sciences, 2023. **13**(1): p. 322-343.
21. COSO, Committee of the Sponsoring Organizations of the Treadway Commission, *COSO Enterprise Risk Management-Integrated Framework Update, URL: http://www.coso.org/ermupdate.html*. 2014.



© 2025 York Partners (Publishing) LLC

22. ISO, International Organization for Standardization, *ISO 22313, Societal security — Business continuity management systems — Guidance (ISO Standard No. 22313:2020). ISO.* https://www.iso.org/standard/75107.html. 2020.
23. GFSI, Global Food Safety Initiative, *The GFSI Benchmarking Process Handbook Version 2024.* GFSI Website, 2024.
24. BRC, (British Retail Consortium) Global Standards, *BRC Global Standard Food Safety, Issue 8, August 1, 2018, URL: https://www.brcbookshop.com/bookshop/brc-global-standard-food-safety-issue-8/c-24/p-414*. 2018.
25. SQF Institute. *SQF Code*. 2012 [cited 2012; Available from: http://www.sqfi.com/wp-content/uploads/SQF-Code-Ed-7-Final-8-13-12.pdf.
26. IFS, International Featured Standards. *IFS Food - Standard for auditing quality and food safety of food products*. 2012 [cited 2012; Available from: http://www.ifs-certification.com/images/ifs_standards/ifs6/IFS_Food_V6_en.pdf.
27. FSSC, Foundation for Food Safety Certification. *Food Safety System Certification 22000 - FSSC 22000, Certification scheme for food safety systems in compliance with ISO 22000: 2005 and technical specifications for sector PRPs*. 2011 [cited 2012; Available from: http://www.fssc22000.com/downloads/FSSC22000changesoktober.pdf.
28. ISO, International Organization for Standardization, *Technical Committee 292 Security and resilience (ISO/ TC 292), Home Page, URL: https://www.iso.org/committee/5259148.html*. 2018.
29. ISO, International Organization for Standardization, *ISO 22331, International Organization for Standardization. (2018). Societal security — Business continuity management systems — Guidelines for people aspects of business continuity (ISO/TS Standard No. 22331:2018). ISO.* https://www.iso.org/standard/50068.html. 2018.
30. ISO, International Organization for Standardization, *ISO 22318, Societal security — Business continuity management systems — Guidelines for supply chain continuity (ISO/TS Standard No. 22318:2017). ISO.* https://www.iso.org/standard/79000.html. 2017.
31. ISO, International Organization for Standardization, *ISO 22317, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA) (ISO/TS Standard No. 22317:2021). ISO.* https://www.iso.org/standard/50054.html. 2021.
32. ISO, International Organization for Standardization, *ISO 22316, Security and resilience — Organizational resilience — Principles and attributes. (ISO/TS Standard No. 22316:2017) ISO.* https://www.iso.org/standard/50053.html. 2017.
33. BCI, Business Continuity Institute, *Good Practice Guidelines (2021) - The Global Guide to Good Practice in Business Continuity: Details the best practices in BCM, strategy development, and planning.* https://www.thebci.org/. 2021.
34. Herbane, Brahim, *Small business research: Time for a crisis-based view.* International small business journal, 2010. **28**(1): p. 43-64.
35. Smith, David, *Business continuity and crisis management.* Management Quarterly, 2003. **44**(1): p. 27-33.
36. Van Der Vegt, Gerben S, Peter Essens, Margareta Wahlström, and Gerard George, *Managing risk and resilience*. 2015, Academy of Management Briarcliff Manor, NY. p. 971-980.
37. McManus, Sonia, Erica Seville, John Vargo, and David Brunsdon, *Facilitated process for improving organizational resilience.* Natural hazards review, 2008. **9**(2): p. 81-90.
38. Bhamra, Ran, Samir Dani, and Kevin Burnard, *Resilience: the concept, a literature review and future directions.* International journal of production research, 2011. **49**(18): p. 5375-5393.
39. Spink, John W, *Chapter 15 Supplement: Foundations of Incident Management and Operational Resilience, Supply Chain Management Introduction: Sourcing, Operations & Logistics, York Partners LLC (Publishing), www.SCMintro.com*. 2025.
40. COSO, Committee of Sponsoring Organizations of the Treadway Commission, *Fraud Risk Management Guide, COSO Publication, Washington, DC, URL: https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf*. 2016.



© 2025 York Partners (Publishing) LLC 

41. COSO, Committee of the Sponsoring Organizations of the Treadway Commission, *Internal Controls – Integrated Framework, URL: http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf*. 2013.
42. COSO, Committee of Sponsoring Organizations of the Treadway Commission, *Applying the COSO ERM Framework. https://www.coso.org/erm-framework, https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf*. 2020.
43. COSO, Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrating with Strategy and Performance, https://www.coso.org/enterprise-risk-management*. 2018.
44. COSO, Committee of Sponsoring Organizations of the Treadway Commission, *Risk Assessment in Practice - Enterprise Risk Management*. 2012, Committee of Sponsoring Organizations of the Treadway Commission, COSO.
45. ISO, International Organization for Standardization, *ISO 22300:2018(en) Security and resilience — Vocabulary, URL: https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en*. 2018.
46. ISO, International Organization for Standardization, *ISO 22000:2018 - Food safety management systems -- Requirements for any organization in the food chain URL: https://www.iso.org/standard/65464.html*. 2018.

/END/


© 2025 York Partners (Publishing) LLC