Chapter 15 Supplement: Foundations of Incident Management and Operational Resilience

John W SPINK, Ph.D.

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

Reference: SPINK, John W (2025). Chapter 15 Supplement: Foundations of Incident Management and Operational Resilience, Supply Chain Management Introduction: Sourcing, Operations & Logistics, York Partners LLC (Publishing), www.ScmIntro.com.

September 2025

Summary

This document explains how incident management and operational resilience form a unified framework for managing disruptions and ensuring business continuity. Incident management provides the *tactical system* for detecting, responding to, and learning from events, while operational resilience supplies the *strategic capability* to sustain essential functions. Both follow the *Plan–Do–Check–Act* cycle (e.g., quality management or the "Deming Wheel"), emphasizing prevention, rapid recovery, and continuous improvement. The document also clarifies terminology that "incident management" and "operational resilience" are the globally recognized terms used in ISO and other industry standards. These activities support the boards of directors, who are ultimately accountable for setting risk tolerance, maintaining competence, and ensuring integrated systems exist to protect stakeholders and maintain trust. Together, these disciplines promote proactive governance, efficient recovery, and adaptive learning across the supply chain.

Key Learning Objectives:

- Define and distinguish incident management and operational resilience.
- Apply resilience principles within incident management frameworks.
- Understand board-level expectations for risk governance and preparedness.

Overview of Incident Management

Incident management is a structured, organization-wide process for identifying, assessing, responding to, and learning from events that disrupt normal operations. Within integrated supply chain management, incident management ensures that disruptions—such as safety issues, cyberattacks, or logistics failures—are contained and resolved through coordinated communication and decision-making. The process supports operational resilience by applying systematic frameworks like the *Plan–Do–Check–Act* cycle (e.g. quality management or the "Deming Wheel"), to maintain essential functions and restore performance efficiently (Figure 1).

- **Definition: Incident management** is the coordinated process of detecting, analyzing, and responding to events that threaten operational continuity and organizational objectives.
- **Application to Operational Resilience:** Effective *incident management* integrates with supply chain risk management and enterprise systems to prevent recurrence, ensuring rapid recovery and continuous improvement, which is *operational resilience*.
- **Board Expectations:** Boards of directors are responsible for setting risk tolerance and ensuring competent, documented incident management and resilience plans exist to prevent surprises and maintain stakeholder confidence.

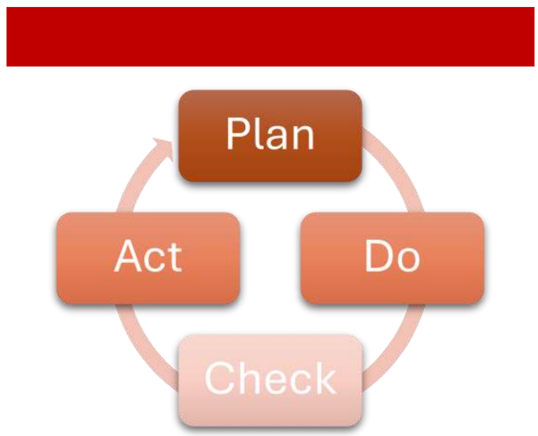

Figure 1 Plan-Do-Check-Act (PDCA) Cycle

The term "incident management" is the correct and preferred term for this scope. **"Incident management"** (two words) is the internationally standardized and widely accepted term across industries, regulations, and management systems.

Theoretical Foundation:

- **Standards usage:**
    - ISO 22320 (*Security and Resilience – Emergency Management – Guidelines for Incident Management*) defines it as the *structured approach to direct, control, and coordinate response and recovery activities following an incident*.

    - ISO 22000 (food safety management), ISO 27035 (information security), and food safety standards refer to *incident management systems* (IMS), not *incident response* or *incident handling*.
- **Industry application:**
    - In business continuity, food safety, cybersecurity, and supply chain risk, *incident management* covers the full lifecycle—preparation, detection, response, recovery, and review—not just the reactive phase.
    - Incident response is a subset of incident management, typically focused only on the immediate containment or mitigation steps.
- **Conceptual focus:**
    - *Incident management* aligns with continuous improvement and resilience frameworks (e.g., the Plan–Do–Check–Act model).
    - It encompasses people, processes, and communications, not just the technical fix.

In Summary:

- Use incident management for enterprise-wide planning and coordination.
- Use incident response only when describing the tactical, front-line actions taken during an event.

Overview of Operational Resilience

Operational resilience is the adaptive capacity of an organization to anticipate, prepare for, respond to, and recover from disruptions while maintaining critical operations. According to ISO 28002, **resilience** is "the ability of an organization to prevent or resist being affected by an event or to return to an acceptable level of performance in an acceptable period of time". In supply chain contexts, resilience extends beyond internal operations to include suppliers and customers, emphasizing adaptability, learning, and communication during crises.

- **Definition: Operational resilience** is the capacity to maintain core functions and recover effectively amid internal or external disruptions.
- **Application to Incident Management:** Incident management systems are reinforced by *operational resilience* strategies and use resilience planning to mitigate disruptions, applying the *Plan–Do–Check–Act* framework for prevention, response, and recovery.
- **Board of Directors' Expectations:** Boards are responsible for defining the organization's risk tolerance, ensuring competent systems and resilience plans are in place to manage disruptions and protect stakeholder interests.

Theoretical Foundation:

- **Standards usage:** ISO 22316 (*Security and Resilience – Organizational Resilience*) and ISO 28002 both use *operational resilience* to describe the ability of an organization to continue delivering critical operations under disruption.
- **Industry and regulatory alignment:** In the financial, food, and infrastructure sectors, regulators (e.g., the UK FCA, US Federal Reserve, and food safety standards) consistently refer to *operational resilience* programs, not *operations resilience*.
- **Conceptual focus:** "Operational resilience" emphasizes the *outcome*—the resilience *of operations and systems*—whereas "operations resilience" sounds narrower, as if referring only to manufacturing or process control.

In Summary:

- Use operational resilience when referring to enterprise-wide capability (covering people, processes, systems, and supply chains).
- Reserve operations resilience only if you're describing a subset focused on manufacturing or process performance.

Intersection of Incident Management and Operational Resilience

Incident management and operational resilience are complementary disciplines—each reinforcing the other within an integrated risk management framework. *Incident management* provides the *tactical response system*—detecting, containing, and resolving specific events that disrupt operations—while *operational resilience* provides the *strategic capability* that ensures the organization can continue delivering essential functions despite those disruptions.

Operational resilience depends on effective incident management to generate data, lessons learned, and process improvements that strengthen preparedness and adaptability. Conversely, incident management is guided by the principles of resilience: anticipating threats, defining risk tolerances, and ensuring critical operations can be maintained within acceptable limits.

In practice, the relationship is cyclical: incident management identifies vulnerabilities and feeds recovery insights into resilience planning; operational resilience frameworks set the standards and competencies that define a successful incident response. Together, they ensure that disruptions are not only managed efficiently but also converted into long-term improvements in continuity, governance, and stakeholder confidence.

Conclusion – Key Takeaways

Building competence in both *incident management* and *operational resilience* requires alignment between planning, execution, and governance. These are most efficient when within a PDCA cycle (Figure 2). The integration of these disciplines strengthens a company's ability to anticipate, respond to, and learn from disruption while maintaining stakeholder confidence and compliance with standards. Organizations should view resilience as an ongoing strategic capability—not a one-time project.

Key Takeaways:

- **Institutionalize Integration:** Develop a unified framework where incident management data, lessons learned, and corrective actions feed directly into operational resilience planning and review cycles.
- **Embed Accountability:** Ensure the board of directors and executive leadership define risk tolerance, oversee response readiness, and regularly test competence through audits, simulations, and after-action reviews.
- **Promote Continuous Learning:** Apply the *Plan–Do–Check–Act* model to every incident, using each event as an opportunity to improve resilience maturity, cross-functional coordination, and communication effectiveness across the supply chain.

References:

Spink (2020). Supply Chain Management Introduction, www.SCMintro.com

McGraw-Hill (2024). Introduction to Supply Chain Management (Sourcing, Operations, and Logistics), https://www.mheducation.com/

OpenAI. (2025, October 20). ChatGPT [Large language model] [Personal communication]. https://chat.openai.com/

/END/ (v3)/