

Strategic Use Case Library

Business Continuity & Crisis Management

**From Static Recovery Plans to Intelligent
Operational Resilience Coordination**



Last Update: February 2026

Contents

1	Executive Overview.....	3
2	Business Challenge.....	4
2.1	Current-State Reality	4
3	Strategic Objective.....	4
4	Target Operating Model	5
4.1	Enterprise Operational Resilience Framework	5
5	Enterprise Implementation Approach	5
5.1	Phase 1 - Resilience Discovery & Operational Assessment	5
5.1.1	Activities	5
5.1.2	Outcome	6
5.2	Phase 2 - Continuity Workflow & Crisis Enablement.....	6
5.2.1	Activities	6
5.2.2	Outcome	6
5.3	Phase 3 - Integration & Continuous Monitoring Activation	6
5.3.1	Example Integrations.....	6
5.3.2	Outcome	6
6	Practical Workflow Scenario	7
6.1	Business Continuity & Crisis Lifecycle Journey	7
6.1.1	Step 1 - Operational Disruption Detection.....	7
6.2	Step 2 - Crisis Activation & Classification.....	7
6.3	Step 3 - Cross-Functional Recovery Coordination	7
6.4	Step 4 - AI-Assisted Resilience Intelligence.....	8
6.5	Step 5 - Recovery Monitoring & Operational Restoration	8
6.6	Step 6 - Executive Crisis & Resilience Visibility	9
7	AI & Intelligence Layer	9
7.1	AI-Driven Continuity & Resilience Capabilities.....	9
8	Executive Visibility.....	9
8.1	Real-Time Operational Resilience Dashboards	9
9	Business Outcomes	10
10	Strategic Value	10
11	Closing Positioning	11

1 Executive Overview

Modern organizations operate in environments where disruptions can emerge at any moment from:

- Cyberattacks
- Technology outages
- Third-party failures
- Supply-chain disruptions
- Regulatory incidents
- Human errors
- Infrastructure failures
- Natural disasters
- Geopolitical events

Despite growing operational dependency and interconnected ecosystems, many organizations still manage business continuity through:

- Static documents
- Manual escalation trees
- Spreadsheet-based recovery tracking
- Isolated crisis teams
- Periodic testing exercises
- Fragmented communication channels

As a result, organizations often struggle to coordinate response activities effectively during real operational disruptions.

This use case demonstrates how enterprises can transform traditional Business Continuity Management (BCM) into a centralized, intelligent, and continuously operating resilience capability powered by automation, workflows, AI-driven intelligence, and real-time executive coordination.

2 Business Challenge

2.1 Current-State Reality

The organization operates across multiple business units, systems, vendors, facilities, and operational environments.

Existing continuity and crisis-management challenges include:

Challenge	Operational Impact
Static BCP documents	Limited operational usability during crises
Manual crisis coordination	Slow response and recovery
Disconnected recovery teams	Poor cross-functional alignment
Limited operational visibility	Delayed executive decisions
Inconsistent escalation procedures	Increased operational confusion
Weak dependency mapping	Hidden critical exposure
Reactive continuity exercises	Limited organizational readiness
Lack of centralized resilience intelligence	Reduced operational resilience

3 Strategic Objective

The objective is to establish a centralized operational resilience and continuity capability that enables:

- Real-time crisis coordination
- Centralized continuity governance
- Cross-functional operational orchestration
- Automated escalation and communication
- AI-assisted resilience intelligence
- Continuous resilience monitoring
- Executive-level operational visibility
- Faster business recovery and continuity execution

4 Target Operating Model

4.1 Enterprise Operational Resilience Framework

The organization establishes a centralized resilience operating model covering:

Component	Description
Business Continuity Governance	Centralizes continuity governance across critical business services, recovery plans, crisis teams, vendors, facilities, operational dependencies, technology environments, and communication structures.
Critical Service Dependency Mapping	Maps critical services, applications, infrastructure, vendors, teams, data dependencies, and recovery priorities to create enterprise-wide resilience visibility.
Crisis Coordination and Escalation	Orchestrates crisis activation, stakeholder notifications, escalation routing, recovery coordination, executive communication, task management, and decision workflows.
Continuous Resilience Monitoring	Continuously monitors resilience through incident intelligence, SLA disruptions, system outages, vendor exposure, operational KPI degradation, crisis indicators, and recovery readiness metrics.
Executive Resilience Intelligence	Provides leadership with real time visibility into disruption impact, recovery progress, service availability, organizational readiness, crisis escalation status, and regional or national exposure.

5 Enterprise Implementation Approach

5.1 Phase 1 - Resilience Discovery & Operational Assessment

5.1.1 Activities

- Business impact analysis (BIA)
- Recovery dependency mapping
- Existing BCP review
- Crisis governance assessment
- Operational resilience maturity analysis
- Stakeholder workshops
- Critical service prioritization

5.1.2 Outcome

A unified operational resilience framework aligned with enterprise continuity and recovery objectives.

5.2 Phase 2 - Continuity Workflow & Crisis Enablement

5.2.1 Activities

- Crisis workflow configuration
- Recovery orchestration setup
- Escalation hierarchy implementation
- Communication workflow automation
- Recovery task management
- Executive dashboard setup
- SLA and RTO/RPO alignment

5.2.2 Outcome

A centralized operational resilience coordination environment.

5.3 Phase 3 - Integration & Continuous Monitoring Activation

5.3.1 Example Integrations

Integration Type	Purpose
IT Monitoring Platforms	Infrastructure outage visibility
SIEM & Security Systems	Cyber disruption intelligence
ERP Platforms	Operational impact monitoring
Vendor Platforms	Third-party continuity visibility
Communication Systems	Crisis notification orchestration
Facility & Infrastructure Systems	Physical operational monitoring

5.3.2 Outcome

Connected and continuously monitored operational resilience intelligence.

6 Practical Workflow Scenario

6.1 Business Continuity & Crisis Lifecycle Journey

6.1.1 Step 1 - Operational Disruption Detection

Disruptions are identified through:

- System outages
- Cybersecurity incidents
- Vendor disruptions
- Operational failures
- Infrastructure alerts
- Compliance events
- Facility incidents
- Regional or geopolitical events

The platform automatically evaluates operational impact.

6.2 Step 2 - Crisis Activation & Classification

The platform automatically determines:

- Severity level
- Affected services
- Recovery priorities
- Stakeholder involvement
- Escalation requirements
- Regulatory implications
- Business continuity impact

Crisis workflows are triggered automatically.

6.3 Step 3 - Cross-Functional Recovery Coordination

The platform coordinates:

- Crisis management teams

- Recovery task assignments
- Stakeholder communications
- Vendor engagement
- Operational restoration workflows
- Executive updates
- Escalation management

All activities remain centrally tracked and traceable.

6.4 Step 4 - AI-Assisted Resilience Intelligence

AI capabilities assist with:

- Crisis summarization
- Dependency impact analysis
- Recovery prioritization
- Operational exposure analysis
- Similar incident correlation
- Escalation recommendations
- Executive resilience summaries

This improves coordination and accelerates recovery decisions.

6.5 Step 5 - Recovery Monitoring & Operational Restoration

The platform continuously tracks:

- Recovery progress
- Critical service restoration
- SLA recovery timelines
- Recovery bottlenecks
- Outstanding operational exposure
- Vendor restoration activities
- Escalation status

Critical delays automatically escalate to leadership.

6.6 Step 6 - Executive Crisis & Resilience Visibility

Executives gain visibility into:

- Crisis status
- Recovery progress
- Operational exposure
- Critical service availability
- Recovery timelines
- Business impact analysis
- Organizational resilience posture
- Strategic continuity readiness

7 AI & Intelligence Layer

7.1 AI-Driven Continuity & Resilience Capabilities

AI Capability	Business Value
Crisis summarization	Faster executive understanding
Dependency impact analysis	Better operational awareness
Recovery prioritization	Faster restoration activities
Operational exposure intelligence	Improved resilience visibility
Similar incident analysis	Faster recovery decision-making
Escalation intelligence	Better coordination
Executive resilience insights	Enhanced strategic oversight

8 Executive Visibility

8.1 Real-Time Operational Resilience Dashboards

Leadership gains centralized visibility into:

- Active crises and disruptions
- Critical service availability
- Recovery progress status
- SLA and RTO performance
- Operational bottlenecks

- Vendor disruption exposure
- Organizational resilience indicators

Enterprise continuity readiness

This transforms business continuity from static documentation into a live operational resilience capability.

9 Business Outcomes

Outcome Area	Impact
Crisis Response	Faster and more coordinated recovery
Operational Visibility	Real-time resilience intelligence
Governance	Centralized continuity coordination
Accountability	Clear recovery ownership
Resilience	Improved operational readiness
Executive Oversight	Better crisis decision-making
Risk Reduction	Earlier disruption identification
Scalability	Enterprise-wide resilience consistency

10 Strategic Value

This transformation enables organizations to evolve from document-based continuity programs into intelligent operational resilience ecosystems.

The organization gains:

- Faster crisis coordination
- Continuous resilience visibility
- AI-assisted operational intelligence
- Centralized recovery orchestration
- Improved executive oversight
- Better operational readiness
- Stronger organizational resilience
- Continuous continuity governance

11 Closing Positioning

"Business continuity is no longer about maintaining recovery documents. It is about continuously coordinating operational resilience across the enterprise in real time."

This use case demonstrates how organizations can operationalize business continuity and crisis management through centralized workflows, AI-driven resilience intelligence, automated coordination, and real-time executive visibility.