

EXECUTIVE BRIEFING 17

Business Continuity in an Uncertain World

Building the organizational capacity to sustain critical operations through disruption, uncertainty and cascading risk.

PRIORITIZE Critical services	PREPARE Response options	ADAPT Operate through disruption	RECOVER Restore & learn
---------------------------------	-----------------------------	-------------------------------------	----------------------------

EXECUTIVE PREMISE

Business continuity is not a binder for rare emergencies. It is the enterprise capability to keep the most important products, services and obligations operating when normal assumptions fail. Resilience begins by deciding what must continue, what can pause and what dependencies could prevent recovery.

Executive Summary

Modern disruption rarely respects organizational boundaries. Cyber incidents can interrupt operations; severe weather can affect facilities and suppliers; geopolitical events can constrain logistics; telecommunications or cloud outages can remove critical technology; and a single third-party failure can cascade through multiple business services.

Traditional continuity planning often concentrates on individual sites or systems. Executive resilience requires a service-based view: which outcomes matter most to customers, regulators, employees and financial stability, and which people, technology, facilities, suppliers, data and decisions are required to sustain them.

A mature continuity program does not attempt to eliminate disruption. It establishes realistic recovery priorities, alternative operating methods, decision authority and practiced coordination so the organization can absorb shocks without improvising its entire response under pressure.

Disruptions Executives Should Plan Across

- Cyberattack, ransomware or destructive technology failure affecting critical services.
- Loss of a facility, utility, telecommunications service, cloud platform or key technology provider.
- Supplier failure, logistics disruption or geopolitical restrictions affecting essential inputs.
- Workforce unavailability, civil disruption, severe weather or public-health events.
- Multiple simultaneous failures that exceed assumptions built into individual recovery plans.

Executive Takeaways

1. Protect services, not assets

2. Know the dependencies

3. Set tolerances

4. Practice decisions

5. Design for adaptation

Continuity priorities should reflect business outcomes rather than individual systems.

Critical services fail where hidden people, technology or supplier dependencies fail.

Leadership must define how much disruption the enterprise can accept.

Plans become capability only when people exercise them under realistic pressure.

Resilience requires alternatives when the planned recovery path is unavailable.

The Yakamichi Enterprise Continuity Framework

- 1. Critical Service Identification** Define the products, services, obligations and decision functions whose prolonged interruption would create material harm.
- 2. Impact & Tolerance** Establish acceptable disruption levels, recovery priorities and the operational consequences as outages extend.
- 3. Dependency Mapping** Map people, facilities, technology, data, suppliers, utilities and decision authorities required to deliver each critical service.
- 4. Continuity Strategies** Develop practical alternatives such as remote operations, alternate suppliers, manual processes, secondary locations and technology recovery.
- 5. Crisis Coordination** Connect continuity plans to executive crisis management, incident response, communications and stakeholder obligations.
- 6. Exercise & Improvement** Test assumptions through realistic scenarios, capture failures and assign remediation until resilience improves.

Service Resilience Model

Question	Executive Meaning	Required Output
What must continue?	Identify critical business services.	Prioritized service catalogue
How long can it fail?	Define tolerable disruption.	Impact and recovery thresholds
What does it depend on?	Reveal concentration and single points of failure.	Dependency map
What if recovery fails?	Prepare alternate operating options.	Continuity strategies

The Dependency Problem

A service may appear resilient because its primary technology is redundant while remaining dependent on one specialist employee, one telecommunications carrier, one supplier, one identity platform or one building utility. Dependency mapping exposes these hidden concentrations before disruption does.

Board and Executive Responsibilities

- Which business services would create material harm if unavailable for one hour, one day or one week?
- Has leadership explicitly approved disruption tolerances and recovery priorities?
- Which suppliers, cloud platforms, facilities or specialist roles represent concentration risk?
- Do continuity plans remain workable when primary technology is unavailable?
- Can critical operations continue if normal communication channels or headquarters are inaccessible?
- Are regulatory, customer and contractual continuity obligations understood?
- Do exercises test cascading failures rather than comfortable single-system scenarios?

Common Continuity Failure Patterns

Plan without capability	Documents exist but teams have not practiced the decisions and workarounds.
Asset-centric recovery	Systems recover according to technical priorities that do not match business-service needs.
Hidden concentration	Multiple critical services rely on the same supplier, platform, location or specialist.
Unrealistic assumptions	Plans assume people, communications or alternate sites will be available when they may not be.
Recovery without coordination	Technology, operations, communications and executive teams restore independently.

Executive Metrics

Useful measures include critical services with approved tolerances, dependency maps completed, recovery strategies validated, concentration risks above appetite, overdue continuity remediation, exercise participation, time achieved in recovery tests, supplier resilience coverage and recurring exercise findings.

180-Day Executive Action Plan

0–30 DAYS | Define what matters

Identify critical business services and assign accountable executive owners.

31–60 DAYS | Set tolerances

Approve disruption thresholds, recovery priorities and minimum service levels.

61–90 DAYS | Map dependencies

Identify critical people, technology, data, facilities, suppliers and concentration risks.

91–120 DAYS | Validate continuity options

Test alternate processes, technology recovery, supplier alternatives and crisis communications.

121–180 DAYS | Exercise cascading disruption

Run an executive scenario involving multiple failures and track corrective actions to closure.

Executive Checklist

- ☐ Critical business services identified
- ☐ Executive service owners assigned
- ☐ Disruption tolerances approved
- ☐ People, technology and supplier dependencies mapped
- ☐ Concentration risks reported to leadership
- ☐ Alternate operating strategies documented
- ☐ Technology recovery aligns with business priorities
- ☐ Crisis communications integrated with continuity plans
- ☐ Critical suppliers included in resilience assurance
- ☐ Executive continuity exercise completed within 12 months

Yakamichi Perspective

Resilience is not the ability to predict the next disruption. It is the ability to continue making good decisions when the disruption is different from the one you planned for.

Organizations become more resilient when continuity is designed around critical services, real dependencies and practiced executive choices rather than optimistic assumptions.

REQUEST A CONFIDENTIAL CONSULTATION

United States: +1 202 413 3763 | Maryland, USA

Nigeria: +234 811 095 0651 | Abuja, Nigeria

YAKAMICHI • Artificial Intelligence • Cybersecurity • Counter-Surveillance • Corporate Risk Intelligence