CONTINUITY HUB

BCP Pillars Quick Card: The Discipline on One Card

FREE FIELD QUICK REFERENCE

Current version — Oct 31, 2026. Update history: https://continuityhub.org/business-continuity-planning-complete-professional-guide/

What is Business Continuity Planning? Deciding, in advance, how an organization keeps its critical work running — or gets it running again fast — when a site, system, supplier, or group of people becomes unavailable. It is not an IT backup document or an auditor binder; it is a governed program with an executive owner. A workable plan is built *function by function* (e.g., "Payroll must run within 3 days, with 2 named people from anywhere using a manual process"), not department by department.

1. THE 5 CORE QUESTIONS EVERY PLAN MUST ANSWER

1. Priority

Which functions cannot wait? Identifies essential operations whose downtime causes immediate failure.

2. Tolerance

How long down? Sets tolerable limit before damage (financial/regulatory) becomes unacceptable (MTPD & RTO).

3. Workaround

What do we do instead? Manual workarounds, alternate site, second supplier, or cross-trained staff.

4. Command

Who decides & acts? Named owners and alternates with authority to declare and execute at 3 a.m.

5. Return

How stand down? Data reconciliation, return to normal operations, and feeding lessons into the plan.

2. THE FOUR PILLARS OF BUSINESS CONTINUITY

A widely used framing to check that a program is complete rather than a set of certification requirements. A program strong in one pillar and missing another is a known shape of failure.

PILLAR	OPERATIONAL FOCUS	KEY ACTIVITIES & DELIVERABLES	FAILURE MODE IF MISSING
1. Prevention & Mitigation	Reducing the chance and size of a disruption before it happens.	Fixing single points of failure, maintaining equipment, hardening systems, and selecting suppliers with their own verified resilience. Lowers how often the plan is needed.	**Frequent Outages:** Plan is overworked; routine failures escalate needlessly.
2. Preparedness	The building work completed *before* the event occurs.	Business Impact Analysis (BIA), risk assessments, written function playbooks, staff training, contact trees, pre-agreed alternate sites & backup vendors.	**Improvisation:** Nothing exists to execute; cannot be created during an active crisis.
3. Response	Execution under command during the first critical hours.	Detecting and declaring the disruption, activating the plan, accounting for people, communicating (staff, customers, regulators), executing initial workarounds.	**Paralysis:** Responders freeze; uncoordinated decisions amplify damage.
4. Recovery	Restoring normal operations and closing the event.	Returning to primary site or system, reconciling data and transactions handled manually, and writing lessons learned directly back into the plan.	**Permanent Limp:** Workarounds become permanent; uncaptured lessons repeat next crisis.

Critical Takeaway: The Known Shape of Failure

Organizations frequently prevent well but never prepare a workaround, or respond heroically with nothing prepared to execute. Recovery ends when the business is whole again — not when the workaround starts.

3. BUSINESS CONTINUITY VS. DISASTER RECOVERY

The two terms are used interchangeably in casual conversation but must be strictly separated in planning. Disaster recovery is a *subset* of business continuity, not a synonym.

DIMENSION	BUSINESS CONTINUITY (BC)	DISASTER RECOVERY (DR)
Primary Focus	**The Business:** Keeping critical functions operating throughout disruptions.	**Technology:** Restoring IT systems, databases, and network infrastructure.
Unit of Analysis	**The Function & its Deadline:** Invoicing, dispensing, shipping, support, payroll.	**The System & its Recovery Time:** Servers, virtual machines, storage, networks.
Operational Scope	People, workarounds, alternate facilities, manual processes, supplier substitutions.	Backups restored, systems rebuilt, cloud failover, services reconnected.
Relationship	The governing umbrella program owned by executive leadership and business functions.	A technical subset supporting the broader business continuity program.
Field Reality	*"What does the order desk do during the 4 hours IT takes to restore the system — and what if IT takes 4 days?"*	*"IT restores database integrity and reconnects application nodes within 4 hours."*

The IT-Only Trap to Refuse:

When a plan is written entirely by IT, it usually contains disaster recovery wearing a continuity title — and goes completely silent on people, premises, and suppliers, which is where most disruptions actually bite.

4. THE 6-STAGE BUSINESS CONTINUITY LIFECYCLE

A continuity program is a repeating cycle, not a one-off project. Programs die when the cycle is run once and treated as finished. The lifecycle *is* the program; the plan document is merely a snapshot.

Stage 1: Policy & Program — FOUNDATIONAL

Executive sponsorship, defined scope (sites, functions, product lines included), assigned roles, and program budget/review rhythm.

Rule: Without executive sponsorship, continuity is a volunteer's hobby.

Stage 2: BIA & Risk Assessment — ANALYTICAL

Identify critical functions, establish impact of outages over time, set MTPD & RTO targets, map dependencies (people, systems, sites, records, suppliers).

Rule: The BIA is the bridge between personal opinion and objective priority.

Stage 3: Strategy Formulation — FINANCIAL

Select recovery methods: alternate sites, remote work, manual workarounds, dual suppliers, cross-trained staff, technology failover.

Rule: Where cost is decided — leadership funds the objective or lowers it honestly.

Stage 4: Plan Development — PROCEDURAL

Draft activation triggers, step-by-step function playbooks, named owners/alternates, contact escalation trees, and pre-drafted comms templates.

Rule: Written for the person holding it at 3 a.m. — short, clear, and actionable.

Stage 5: Exercising — VALIDATION

Tabletop walkthroughs, operational simulations, and live failover tests of real manual workarounds. Fix every deficiency exposed by tests.

Rule: A plan that has never been exercised is merely a hypothesis.

Stage 6: Maintenance & Review — CONTINUAL

Scheduled periodic reviews AND mandatory reviews triggered by material change (new core systems, facilities, staff moves, supplier switches).

Rule: Untested, unmaintained plans rot at a predictable speed.

5. THE THREAT-AGNOSTIC "LOSS-OF-4" FOUNDATION

Fires, floods, cyberattacks, power grid collapses, and pandemics are different causes with identical effects: a function is unavailable. Good plans plan against the *effect*:

1. Loss of Site

Facility locked, flooded, burned, or contaminated.
Response: Relocation to secondary site, pre-arranged remote work, satellite hubs.

2. Loss of System

Ransomware, SaaS outage, server crash, fiber cut.
Response: Manual paper forms, offline spreadsheets, disconnected processing.

3. Loss of People

Severe absenteeism, transit strike, key staff departure.
Response: Named alternates, cross-training matrix, documented step-by-step procedures.

4. Loss of Supplier

Vendor bankruptcy, logistics breakdown, breach.
Response: Pre-contracted secondary suppliers, emergency buffer inventory, alternate parts.

6. PROGRAM ROLES & TESTING CADENCE

Governance Hierarchy

Executive Sponsor	Owns accountability; sets risk appetite, funds strategies, accepts BIA recovery objectives.
BCP Coordinator	Runs the lifecycle engine; schedules BIAs, drives updates, coordinates exercises, tracks fixes.
Function Leaders	Own the playbook content; define realistic workarounds because they know daily operations.
All Responders	Know where plans live offline, maintain current contact details, execute first-hour tasks.

Testing Cadence (Avoid Plan Rot)

Tabletop Walkthroughs	Quarterly or twice/year; facilitated scenario review with role holders; finds stale assumptions.
Functional / Live Tests	Scheduled for critical functions; actual failover or running manual workarounds for real.
On Material Change	Immediate test after new IT systems, facility relocations, reorgs, or new critical vendors.
Findings Review	Mandatory post-exercise remediation log with single-point owners and firm deadlines.

7. ISO 22301 AT A GLANCE

The Management System Standard: ISO 22301 specifies requirements for establishing, operating, maintaining, and improving a Business Continuity Management System (BCMS) using the Plan-Do-Check-Act cycle. It does not provide a plan template or certify a document — certification audits verify that the *management system* actually functions (the BIA is real, plans match the analysis, exercises occur, and findings are fixed). The value is the discipline of the cycle.