ELEVATE
SOLUTIONS

TEMPLATE · BUSINESS & INDUSTRY

Business Continuity Plan Template

People, process, comms

Keep operating during disruption. People, processes, communication, and system dependencies — with worked examples you can replace with your own.

© 2026 Elevate Solutions

00 — BEFORE YOU START

BCP vs. DR — and how to use this template

A business continuity plan (BCP) keeps your operations running when something breaks. A disaster recovery (DR) plan brings your systems back. They are different documents with different owners, and confusing them is the most common reason continuity planning fails.

	BUSINESS CONTINUITY (THIS DOCUMENT)	DISASTER RECOVERY (SEPARATE DOCUMENT)
Question	How do we keep serving clients while X is down?	How do we restore X, and how fast?
Scope	People, workplace, suppliers, communication	Servers, data, applications, backups
Owner	Operations / managing partner / practice lead	IT lead or IT provider
Key metric	Maximum tolerable downtime (MTD) per process	RTO / RPO per system
Output	Workarounds, cascades, holding statements	Restore runbooks, backup test results

This template builds the BCP. Where technology recovery comes up (section 02), the plan points to your DR plan rather than duplicating it. If you do not have a DR plan, note that as a gap on the version page — do not try to make this document do both jobs.

How to use this template

- [ ] **Assign a plan owner** 1
  One named role (not a committee) accountable for completing, testing, and maintaining the plan.
- [ ] **Run the BIA first (section 01)** 2
  Everything else depends on knowing which processes matter most and how long each can be down.
- [ ] **Fill sections 02–03 for Tier 1 and Tier 2 processes only** 3
  Lower tiers get a one-line workaround. Depth where it matters; do not pad.
- [ ] **Test within 90 days of signing (section 04)** 4
  An untested plan is a draft. Schedule the first tabletop before you file the document.

> **KEEP A COPY OFF-NETWORK**
> If the disruption is a cyber incident, your file server and email may be the things that are down. Keep a printed copy and an offline copy (encrypted USB or a separate cloud account) with the plan owner and one deputy.

© 2026 Elevate Solutions

Company _____ Plan owner (role & name) _____ Date adopted _____

01 — BUSINESS IMPACT ANALYSIS

Which processes matter, and how long can each be down

The BIA is an inventory of your business processes — not your systems — ranked by how quickly an outage starts causing real damage. Pull in the people who actually run each process; the owner of a process usually knows its workaround better than management does.

Impact ratings

Rate each process 1–3 in three categories. Use the highest of the three as the overall impact score.

RATING	FINANCIAL	REGULATORY	CLIENT
3 — High	Revenue stops or contractual penalties accrue	Statutory deadline or filing missed; notification duty possible	Client matter, care, or transaction directly harmed
2 — Medium	Revenue delayed; recoverable with effort	Compliance evidence gaps; deadlines at risk past 72 hours	Visible service degradation; clients must be told
1 — Low	Internal cost only	No regulatory exposure	Not client-visible within a week

Prioritization tiers

Tiers translate the BIA into recovery order. The MTD bands below are planning ranges we use as a starting point — adjust to your contractual and regulatory deadlines.

TIER	MAX TOLERABLE DOWNTIME	WHAT IT MEANS
Tier 1	≤ 4 hours	Workaround must start the same business day; pre-staged and rehearsed.
Tier 2	≤ 24 hours	Workaround documented and tested; activated on declaration.
Tier 3	≤ 72 hours	One-line workaround; owner improvises within it.
Tier 4	› 72 hours	Defer until Tiers 1–3 are stable. No plan effort beyond this row.

Process inventory worksheet

One row per process. The first row is a worked example for a generic professional-services firm — replace it with your own. Copy this table until every revenue-bearing, regulated, or client-facing process appears.

PROCESS	OWNER	MTD	SYSTEMS & DEPENDENCIES	MANUAL WORKAROUND	IMPACT (F/R/C)	TIER

Example: Client billing & trust accounting	Finance manager	24 h	Practice mgmt system, bank portal, email	Record time/charges on paper ledger template; process trust transactions at bank branch with two signatories; reconcile on restore	3 / 3 / 2	2

COMMON MISTAKE

Listing systems instead of processes. "Email is down" is a DR problem. "We cannot intake new clients because intake runs on email" is the BCP problem — and it has a workaround (a phone script and a paper intake form) that no IT plan will give you.

02 — RECOVERY STRATEGIES

Per-tier strategies: people, workplace, technology, suppliers

For each Tier 1 and Tier 2 process, decide in advance how work continues across four domains. Write the decision, not a discussion of options.

People

Every critical process needs at least one trained alternate. "Trained" means they have done the task in the last six months, not that they sat near someone who does it.

CRITICAL ROLE / TASK	PRIMARY	ALTERNATE	PROCEDURE DOCUMENTED AT	LAST CROSS-TRAINED
Example: Payroll submission	Office manager	Finance manager	Ops handbook §4, payroll portal runbook	Mar 2026

Remote-work activation. Define the trigger ("office inaccessible or unsafe; declared by plan owner"), confirm every Tier 1/2 role has a laptop and MFA-protected remote access that works from home today, and state where the staff roster with personal phone numbers lives offline.

Offline staff roster location _____

Workplace

Choose one primary strategy per scenario before the event. Most firms under 100 staff choose work-from-home as the default and reserve paid space for functions that genuinely need a desk (reception, mail intake, physical files).

OPTION	USE WHEN	PRE-WORK REQUIRED
Work from home (default)	Office loss with intact staff and systems	Equipment + remote access verified per person; see People above
Split / partial occupancy	Office partially usable; client-facing functions on site	Decide which roles return first; building contact on cascade
Serviced office / day space	Outage past 2 weeks, or functions that need a desk	Identify two nearby providers; know booking lead time and cost
Reciprocal space (peer firm)	Short-term, small team, existing relationship	Written agreement; confidentiality reviewed by counsel

Default workplace strategy _____ **Backup space provider & contact** _____

Technology — pointer to the DR plan

System restoration is the DR plan's job. The BCP needs only three things: where the DR plan lives, who executes it, and the agreed RTO/RPO for the systems behind your Tier 1 and Tier 2 processes — so the workarounds above are sized to a known gap. If the DR plan's RTO for a system is 24 hours and the process MTD is 4 hours, the workaround carries the difference; that gap is the whole point of this document.

DR plan location (offline copy) _____ **DR executor (IT lead / provider + phone)** _____

Tier 1 systems RTO / RPO (from DR plan) _____ **Last successful restore test date** _____

Suppliers

List vendors whose failure stops a Tier 1 or Tier 2 process. For each, name an alternate you could switch to inside the MTD — and verify the alternate annually, because "we'd just use X" often turns out to require a contract you do not have.

VENDOR	SERVICE / PROCESS SUPPORTED	TIER	ALTERNATE	SWITCH STEPS / CONTRACT STATUS	LAST VERIFIED
Example: Answering service	Client intake phone line	1	Carrier call-forward to two staff cell phones	Forwarding code documented; tested quarterly	Feb 2026

03 — COMMUNICATION PLAN

Who says what, to whom, on which channel

In a disruption, silence is read as incompetence and improvised messages create liability. Decide the activation rules, the cascade order, and the first two messages now — then the on-the-day job is filling in brackets, not drafting.

Activation

The plan activates when any of the following holds, as judged by the declaring authority — do not wait for certainty:

- ☐ **A Tier 1 process is stopped, or expected to stop within its MTD** 1
- ☐ **The office is inaccessible or unsafe** 2
- ☐ **A confirmed or suspected cyber incident affects production systems** 3
  Run this plan and the incident-response plan in parallel; IR leads on containment, BCP leads on operations and comms.
- ☐ **A critical vendor declares an outage past your MTD** 4

Declaring authority (role) _____ **Deputy (if unreachable in 30 min)** _____

Contact cascade

AUDIENCE	WHEN	CHANNEL	OWNER	CONTACT LIST LOCATION
Staff	Hour 0–1	Out-of-band (below)	Plan owner	
Insurer (cyber/property)	Hour 0–2	Carrier hotline	Declaring authority	
Counsel	Hour 0–2 if cyber or client data involved	Phone	Declaring authority	
Clients (affected first)	Hour 2–8	Phone for top clients, then email/portal	Relationship leads	
Vendors / IT provider	Hour 0–4	Phone / ticket	Ops lead	
Landlord / building	As relevant	Phone	Office manager	

© 2026 Elevate Solutions

OUT-OF-BAND CHANNEL — DECIDE NOW

Assume email and chat are down or compromised; in a cyber incident they may also be read by the attacker. Pick one channel that does not depend on your tenant (SMS broadcast list, signal-style group, or a phone tree), load it with personal numbers, and test it twice a year. Channel chosen: _____

Holding statement — staff

TEMPLATE (SEND VIA OUT-OF-BAND CHANNEL)

Team — at [TIME] today we experienced [ONE-SENTENCE PLAIN DESCRIPTION, e.g. "a building closure" / "an IT systems outage"]. We have activated our continuity plan.

What this means for you: [WORK FROM HOME / REPORT TO ALTERNATE LOCATION / STAND BY]. Do not use [AFFECTED SYSTEMS] until further notice. Direct all client questions to [NAME]; do not speculate about cause or timeline in writing.

Next update by [TIME] from [SENDER] on this channel. — [DECLARING AUTHORITY NAME]

Holding statement — clients

TEMPLATE (TOP CLIENTS BY PHONE FIRST, THEN SEND)

Dear [CLIENT NAME] — we are writing to let you know that [FIRM NAME] is currently managing [A FACILITIES DISRUPTION / A TECHNOLOGY OUTAGE] affecting [SCOPE — keep factual, no cause speculation].

Your matters remain our priority. [DEADLINE/DELIVERABLE STATUS, e.g. "All filings due this week are on track" / "We will confirm the status of your deliverables by [TIME]"]. During this period, please reach us at [PHONE] or [ALTERNATE EMAIL].

We will update you by [DATE/TIME]. Thank you for your patience. — [RELATIONSHIP LEAD NAME, TITLE]

Media policy: No employee speaks to media or posts about the incident; all inquiries go to _____ (role), who responds only with counsel-approved language.

04 — TESTING & ACTIVATION

Exercise the plan, then keep it alive

Plans decay. Staff change, vendors change, and the workaround that worked last year quietly stops working. A fixed exercise calendar and explicit review triggers are what separate a plan from a binder.

Exercise calendar

EXERCISE	FREQUENCY	PARTICIPANTS	OUTPUT
Tabletop walkthrough	Semiannual	Plan owner, process owners, IT lead/provider	After-action report; plan edits within 30 days
Full test (workarounds live, out-of-band cascade fired)	Annual	All staff (cascade); Tier 1 process teams (workarounds)	Cascade reach %; workaround timings vs. MTD
DR restore test (run by IT — verify, don't run)	Per DR plan	IT lead / provider	Restore evidence filed with this plan

Scenario library

Rotate one scenario per tabletop. The questions are the exercise — answer them against the current plan and log every gap.

SCENARIO	PROMPT QUESTIONS
Ransomware (present in 44% of breaches, up 37% year over year — Verizon DBIR 2025)	Email and file server are encrypted. How does the cascade run without the tenant? Which Tier 1 workarounds function with zero systems? Who calls the insurer, and is the hotline number reachable offline?
Office loss	Building closed indefinitely as of 6 a.m. Who declares, by when is staff notified, what happens to today's client meetings, where does mail and reception go?
Key person	The one person who runs [PROCESS] is unreachable for three weeks. Can the alternate actually execute from the documentation alone? What approvals stall, and who inherits signing authority?
Vendor failure	[CRITICAL VENDOR] declares a multi-day outage. At what hour do you trigger the alternate? Does the switch require contracts, data, or credentials you do not currently hold?

After-action template

Exercise / incident & date _____ **Facilitator** _____

What worked _____

© 2026 Elevate Solutions

Gaps found (plan vs. reality) _____

Plan edits required + owner + due date _____

Plan maintenance — review triggers

Review and re-approve this plan annually, and within 30 days of any of the following:

- ☐ **Staffing change in any role named in this plan** 1
- ☐ **System change behind a Tier 1/2 process (new platform, migration, retirement)** 2
- ☐ **Critical vendor added, replaced, or materially changed** 3
- ☐ **Office move, lease change, or headcount shift > 20%** 4
- ☐ **Any real activation or failed exercise** 5

Version & approval

VERSION	DATE	AUTHOR	CHANGE SUMMARY	APPROVED BY
1.0			Initial adoption	

Approved by (name, title) _____ **Signature** _____ **Next review due** _____

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io

This document is general guidance, not legal advice. Requirements vary by jurisdiction, regulator, and policy — confirm specifics with your counsel, compliance officer, or carrier.