



FREE RESOURCE — BUSINESS CONTINUITY PLAN
TEMPLATE

Business Continuity Plan Template

A practical, audit-ready BCP for UK SMEs. Run a real Business Impact Analysis, set defensible RTO and RPO targets per critical process, document your recovery strategies, capture every contact your team will need at 3 a.m., and keep a real test schedule so the plan still works when you need it.

BIA

BUSINESS
IMPACT
ANALYSIS

AUDIT-READY

RTO

RECOVERY
TIME
OBJECTIVE

MTPD

MAXIMUM
TOLERABLE
PERIOD OF
DISRUPTION

Fillable

TICK & TYPE
IN ANY VIEWER

PREPARED FOR

Cloudswitched Knowledge
Library

PREPARED BY

Cloudswitched Ltd.

VERSION

2026 Edition

FORMAT

Interactive PDF

00

How to use this template

A business continuity plan (BCP) answers one question: **when something disrupts your operation — ransomware, fire, flood, supplier collapse, a long power cut — how do you keep the critical work going and bring the rest back?** This template walks through the six decisions every BCP must make. Fill it in once, keep it under annual review, and rehearse it — a plan never tested is just a document.

AN UNTESTED BCP IS A HOPE, NOT A PLAN

The most common failure mode in a real incident is a BCP that looked credible on paper but had never been walked through end-to-end. Section 05 builds a real test calendar — commit to at least one quarterly tabletop, one annual partial test, and one full plan exercise per year. Record the measured outcome against the RTO and RPO targets you set in Section 02.

The six BCP sections

- **01 Business Impact Analysis** — identify every critical process, score the impact of losing it, and capture dependencies.
- **02 Recovery Targets & Strategies** — commit to a measurable RTO and RPO per critical process, then pick a recovery strategy for each.
- **03 Continuity Procedures** — the step-by-step runbook for invoking the plan, stabilising operations and restoring services.
- **04 Recovery Team & Communication Tree** — who decides, who acts, who tells staff, customers and regulators — with phone numbers.
- **05 Plan Testing & Maintenance** — tabletop, partial and full plan exercises with a real cadence and review log.
- **06 Sign-off & Distribution** — who has approved this BCP, who holds a copy, and when it is next due for review.

Roles to agree before a real incident

- **BCP Commander** — senior decision-maker who invokes the plan, owns escalation, signs off on standing down.
- **Operations Lead** — runs the recovery effort across the critical processes, owns the runbook in Section 03.
- **IT & Systems Lead** — restores systems, data, network and access in line with the RTO/RPO commitments in Section 02.
- **Communications Lead** — staff, customers, suppliers and (where relevant) the ICO and insurer, on a defined cadence.
- **Scribe** — keeps a real-time log so the post-incident review has a factual timeline.

01

Business Impact Analysis

A BIA does two things: list every business process you depend on, and score what happens if each one stops. The output drives everything else — you cannot set credible recovery targets without it. Be honest about impact: scoring everything as “critical” means nothing is critical.

Reference: impact rating scale

RATING	FINANCIAL IMPACT	OPERATIONAL / REGULATORY IMPACT
Critical	> £25k per day of disruption	Statutory breach, contract default, safety risk, brand-defining incident
High	£5k–£25k per day	Significant customer impact, missed SLAs, regulator notifiable
Medium	£1k–£5k per day	Internal disruption, some customer complaints, recoverable
Low	< £1k per day	Inconvenience only, no customer or regulator impact

Critical process register

One row per business process. The Process owner is the person who signs off the impact rating — not the IT lead who has to deliver the recovery.

BUSINESS PROCESS	IMPACT RATING	IMPACT OF DISRUPTION	KEY DEPENDENCIES	PROCESS OWNER

DEPENDENCIES ARE WHERE BIAS USUALLY FAIL

Every critical process depends on something: a system, a key person, a supplier, a building, a network connection. Capture the dependency in the BIA itself — otherwise you build a recovery plan around the process and discover during a real incident that the dependency you forgot was the actual single point of failure.

02

Recovery Targets & Strategies

For every critical process in Section 01, commit to a measurable recovery target and pick a recovery strategy. Targets that look impressive on paper but cost ten times your continuity budget will get quietly missed in a real incident — pick what you can fund and test.

Reference: recovery strategy options

STRATEGY	TYPICAL RTO	WHAT IT MEANS IN PRACTICE
Hot standby	< 1 hour	Fully running replica, automatic failover, continuous data sync
Warm standby	2–8 hours	Pre-built infrastructure, scaled-down, requires manual cut-over
Cold standby	1–3 days	Configuration documented, infrastructure rebuilt on demand from backup
Manual workaround	1–5 days	Process delivered manually / on paper until systems are restored
Suspend service	n/a	Accept the outage; document the trigger and the customer message

Per-process recovery targets

One row per critical process from Section 01. RTO = how fast you must recover; RPO = how much data loss you can absorb; MTPD = the point at which the impact becomes existential.

BUSINESS PROCESS	RTO TARGET	RPO TARGET	MTPD	RECOVERY STRATEGY	STRATEGY OWNER

RTO, RPO AND MTPD — THE DIFFERENCE MATTERS

RTO = maximum acceptable time to bring a process back. **RPO** = maximum acceptable data loss measured in time. **MTPD** = the point beyond which the impact threatens the business itself. RTO must be tighter than MTPD — if not, the strategy must change, not the number.

03

Continuity Procedures

The runbook for invoking the BCP, stabilising the operation and restoring critical processes. Work top-down; do not skip a step because it “looks fine”. Tick each item as it completes, and have the BCP Commander confirm before progressing between phases.

Phase 1 — Invoke & stabilise (first hour)

- ☐ **BCP invoked** by Commander — time, trigger and scope logged by the Scribe.
- ☐ **Recovery team assembled** — Operations, IT, Comms and Scribe on a single bridge.
- ☐ **Safety first** — people accounted for, premises controlled, emergency services contacted if required.
- ☐ **Initial holding statement** issued to staff and key customers — acknowledged, scoped, time of next update.

Phase 2 — Execute recovery (within RTO)

- ☐ **Recovery strategy triggered** per process — the standby, workaround or suspend option chosen in Section 02.
- ☐ **Critical processes restored first** in dependency order — payments / safety / customer-facing before back-office.
- ☐ **Manual workarounds activated** for any process whose system recovery exceeds its RTO.
- ☐ **Communication cadence in force** — staff and customer updates on the schedule in Section 04.
- ☐ **Regulator / insurer notified** if reportable — ICO within 72 hours for personal-data breaches.

Phase 3 — Validate, stand down & review

- ☐ **Service validation** — every critical process confirmed operational by its owner.
- ☐ **All-clear notification** sent to staff, customers and regulators — with any residual limitations called out.
- ☐ **BCP stood down** by the Commander — time and final state recorded by the Scribe.
- ☐ **Post-incident review** scheduled within five business days — actual RTO/RPO and BCP changes.

04

Recovery Team & Communication Tree

In a real incident you do not have time to look up phone numbers — capture every contact you might need now. The recovery team is who runs the BCP from the inside; the communication tree is the cascade for telling everyone else what is happening.

Recovery team

ROLE	PRIMARY NAME	MOBILE	EMAIL	DEPUTY CONTACT
BCP Commander	_____	_____	_____	_____
Operations Lead	_____	_____	_____	_____
IT & Systems Lead	_____	_____	_____	_____
Communications Lead	_____	_____	_____	_____
Scribe	_____	_____	_____	_____
Executive sponsor	_____	_____	_____	_____

Communication tree — external contacts

PARTY	CONTACT / ACCOUNT	PHONE	EMAIL / PORTAL
Cyber insurance	_____	_____	_____
IT support partner	_____	_____	_____
Bank / payment provider	_____	_____	_____
Key supplier / SaaS	_____	_____	_____
Landlord / facilities	_____	_____	_____
ICO (if data breach)	Information Commissioner	0303 123 1113	ico.org.uk/report-breach

DEFINE THE CASCADE UP-FRONT

The Commander tells the Communications Lead; the Comms Lead tells one person per audience — staff (HR/People), customers (Sales/Account Management), suppliers (Procurement), regulators (DPO). Every audience hears from exactly one named voice on a defined cadence (typically every two hours during the active phase). One source of truth prevents the rumour-mill that always kicks off in the first hour.

05

Plan Testing & Maintenance

The single best predictor of recovering successfully in a real incident is how often you have practised. Pick a cadence per test type and stick to it — then record actual measured RTO and RPO against the Section 02 targets.

Reference: minimum recommended cadence

TEST TYPE	CADENCE	WHAT IT PROVES
Tabletop walkthrough	Quarterly	Runbook still reads correctly, team knows their roles, gaps surface on paper
Partial plan test	Twice per year	One critical process actually recovered using its Section 02 strategy
Full plan exercise	Annually	End-to-end exercise across multiple processes, including comms cascade

Next planned test — tick one

☐ Tabletop walkthrough
 ☐ Partial plan test
 ☐ Full plan exercise

Test calendar & results

One row per test executed. Capture the measured outcome — not the planned one.

DATE	TEST TYPE	SCOPE & SCENARIO	RTO MEASURED	RPO MEASURED	PAS FAI

Plan review schedule

REVIEW TYPE	FREQUENCY	NEXT REVIEW DATE	OWNER
Light review	Quarterly		
Full plan review	Annually		
Post-incident review	Within 5 days		

06

Sign-off & Distribution

A BCP without sign-off is a draft. Capture who has approved it, who holds a copy, and when it is next due for review. Without those three answers, accountability evaporates the moment the plan is filed.

Plan metadata

Organisation	_____	Plan version	_____
Effective date	_____	Next review date	_____
Plan owner	_____	Classification	_____

Distribution list

Every role that needs a current copy of the plan. A BCP locked in one inbox is no plan at all.

HOLDER / ROLE	NAME	COPY FORMAT	DATE ISSUED
BCP Commander	_____	_____	_____
Operations Lead	_____	_____	_____
IT & Systems Lead	_____	_____	_____
Communications Lead	_____	_____	_____
Executive sponsor	_____	_____	_____

Approval

PREPARED BY	APPROVED BY	DATE OF APPROVAL
_____	_____	_____

Need cloud backup & continuity built for you?

Cloudswitched designs and runs immutable cloud backup, Azure Site Recovery and a tested BCP for UK SMEs — with measured RTO/RPO, scheduled exercises and 24/7 incident support on a fixed-fee retainer.

info@cloudswitched.com

cloudswitched.com/solutions/cloud-backup



CLOUDSWITCHED

BUSINESS CONTINUITY & CLOUD BACKUP

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom