

BUSINESS CONTINUITY PLANNING (BCP) GUIDE

A practical guide for
New Zealand businesses

June 2026 | Business Canterbury

Contents

About this guide	3
Business Continuity Planning fundamentals.....	3
Introduction: preparing your BCP	6
Plan overview and control	8
Building your Business Continuity Plan	10
1. Assess.....	11
Identify critical business processes.....	11
Identify and map supporting functions for critical business processes	12
Identify disruption scenarios	13
Gather information, assess impact and likelihood, prioritise risk and determine recovery timeframes	15
2. Prepare.....	19
Roles, contacts and delegated authority	19
Dependencies, single points of failure and readiness gaps	20
People, safety and wellbeing	21
Premises, equipment and physical assets.....	21
Technology, systems, data and manual controls.....	22
Key parties and critical providers	23
Financial, insurance, obligations and evidence	23
Communication plan and message templates	24
3. Respond	25
Activation triggers and escalation thresholds	25
Immediate response checklist.....	26
First hour, first day and first week	26
Decision rights, records and recovery actions	27
Scenario response prompts	27
Situation updates and return to normal.....	29
4. Review.....	30
Practical tests	30
After-action review and improvement actions	30
Maintenance cycle and review triggers	31
30 / 60 / 90 day roadmap and readiness checklist	31
Quick references	33

Important use note: The Business Continuity Plan template is the working document. Record business-specific information in the template. Use this guide to make the right decisions, understand the key concepts and check quality before approval.

About this guide

This Business Continuity guide forms part of MBIE Business Resilience training programme, delivered by the Regional Business Partner Network (RBPN).

All information relating to this BCP training is available at [Business.govt.nz](https://business.govt.nz)

This guide helps New Zealand businesses prepare, use and maintain a practical Business Continuity Plan (BCP) so that they have a plan when faced with disruption, before the pressure arrives.

The BCP templates to complete alongside this guide are available for download on the [Business.govt.nz](https://business.govt.nz) website.

This guide explains what each section means and how to complete the BCP template. Use this guide as the reference document while building or improving your plan.

General information reminder: This guide provides general information only. It is not legal, tax, insurance, employment, cyber security, health and safety, financial or other specialist advice. Businesses should check current official guidance and seek appropriately qualified advice where needed.

A Business Continuity Plan is a working plan. It is where the business records ownership, critical processes, roles, contacts, actions, decision records, review records and supporting detail.

A short, current and tested plan is more useful than a long document that cannot be found or understood during disruption.

Business Continuity Planning fundamentals

What a Business Continuity Plan is

A BCP is a preventative practical plan for keeping the most important parts of the business operating, or restoring them quickly, after an unplanned disruption.

It focuses on outcomes that must continue: protecting people, serving priority customers, protecting physical assets, maintaining cash flow, meeting obligations, preserving records and returning to normal operations in a controlled way.

A BCP is made up of five practical components that need business input and decisions:

- Scope and ownership;
- Critical business processes and recovery needs;
- Dependencies and alternative options;
- Roles, delegations and communications;
- Testing, review and maintenance.

Together, these components turn business priorities into clear decisions, actions and recovery steps.

The plan should be specific enough to guide first actions, but not so detailed that it becomes hard to use under pressure.

How a BCP differs from an Emergency Response Plan

An Emergency Response Plan focuses on immediate life safety and site control, such as evacuation, first aid, emergency services, assembly points and urgent safety instructions.

A business continuity plan is broader.

Beyond preparing for an emergency, it provides you with a playbook when any situation arises that impacts on your business, to keep it running through any disruption.

How do we keep serving customers? How do we pay our staff? How do we reach our suppliers? How do we take orders if a system is down? How do we protect our cash and our records?

Area and typical timing	Primary focus	Typical output
Emergency response (during the incident and first minutes)	Life safety, first aid, evacuation and immediate hazards.	Evacuation procedure, emergency contacts, first aid and site control.
Crisis decision-making (first hours and days)	Leadership decisions under uncertainty and stakeholder confidence.	Response lead, decision rights, meeting rhythm and escalation points.
Business continuity (during disruption and recovery)	Continue or restore critical business processes at an acceptable pace and level.	Critical process priorities, practical actions, communication plan and recovery action plan.
Technology recovery (as required by the business)	Restore systems, data, devices, networks and technology services.	System recovery order, provider escalation and backup/access evidence.
Return to normal (days to months)	Clear backlog, reconcile records, finalise claims and improve the plan.	Return-to-normal checklist, after-action review and improvement actions.

The four-part practical framework

The four-part framework helps shape your BCP and is the base approach used to create a plan relevant to your specific business.

It keeps the plan practical: Assess what matters, Prepare the actions, Respond using the plan, and Review so the plan stays current.

To support practical application, each part of the framework is broken down further in the sections below, outlining the key considerations, actions and intended outcomes.

Framework	Main question	Main output
1. Assess	What could go wrong, and what matters most?	Business priorities, critical processes, impact, recovery needs and risk priorities.
2. Prepare	What arrangements are in place before pressure hits?	Roles, contacts, dependencies, practical actions, communication plan, evidence and readiness actions.
3. Respond	What happens in the first hours, days and weeks?	Activation, response team, decision and communication records, recovery action plan and return-to-normal steps.
4. Review	How do we keep the plan current and useful?	Testing, review records, improvement actions, maintenance cycle and readiness checks.

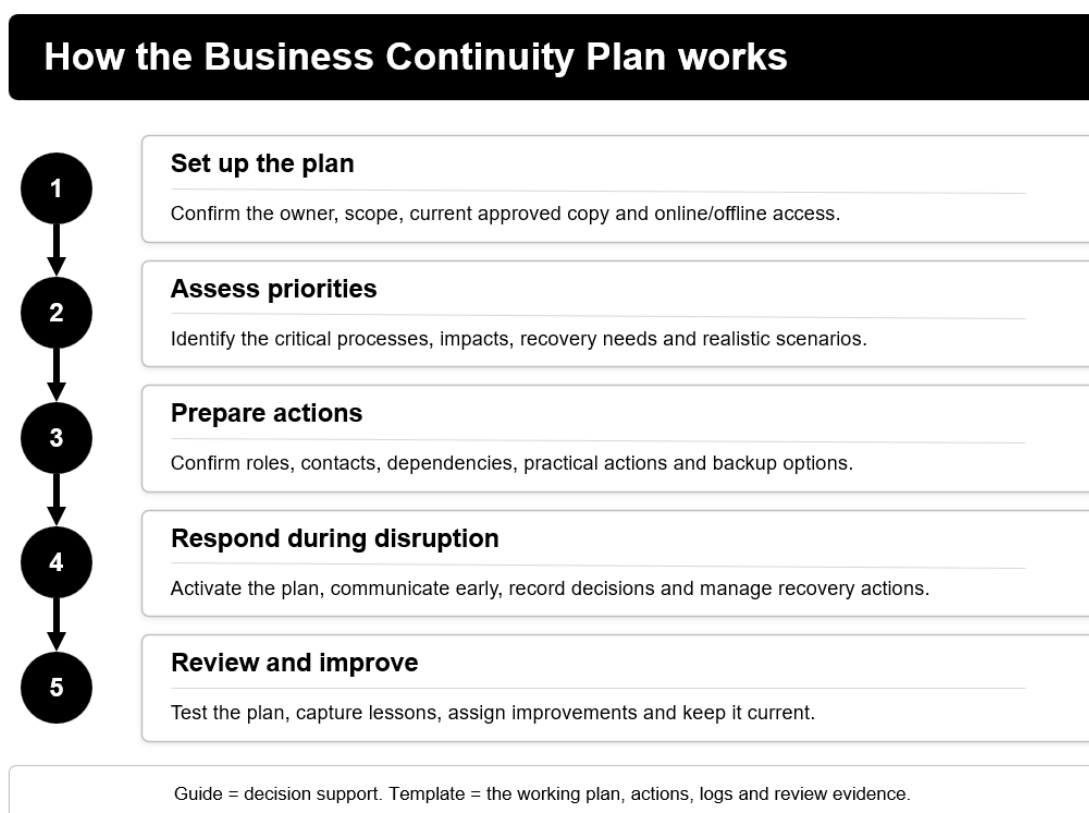
The five questions a good plan answers

1. What could go wrong?
2. What must keep running?
3. Who does what?
4. How do we communicate?
5. How do we recover?

Practical decision: Do not start by listing every possible event. Start by identifying the business outcomes that must continue, then decide what could interrupt them and what practical actions would keep them at a minimum service level.

Introduction: preparing your BCP

Use the steps below after you understand what a BCP is, why it matters and the core parts it should cover. The sequence is designed to produce an initial plan that is useful quickly: name the plan owner, identify critical business processes, record key contacts, confirm response roles, document realistic practical actions and agree how decisions, communications and evidence will be managed.



When identifying critical processes, use the right level of detail.

For example, calibrating a machine is a task; manufacturing and dispatching priority customer orders is a critical business process.

The plan should focus on the processes that protect people, customer commitments, revenue, quality and continuity of supply.

The table below sets out the key components of a BCP, showing where to complete each step in the template and the purpose of each step.

Key components of a Business Continuity Plan

Step	Template section	Purpose / outcome
Confirm ownership and access	Plan overview and control	Name the plan owner, backup owner, approver, current approved copy and offline/offsite access method.
Identify critical processes	1.1A to 1.1C	List the processes that must keep running or be restored first, including minimum operating levels and recovery timeframes.
Rate realistic scenarios	1.2 and 1.3	Identify plausible disruptions, impact, likelihood and the priority risks to prepare for.
Prepare roles and contacts	2.1 and 2.5	Confirm who does what, who can approve urgent decisions and how critical parties will be contacted.
Capture dependencies and gaps	2.2 to 2.6	Identify single points of failure across people, premises, machinery, systems, suppliers, cash flow and authority.
Prepare response tools	2.7 and 3.1 to 3.8	Set up communication templates, activation triggers, checklists, simple records, situation updates and return-to-normal steps.
Test and maintain	4.1 to 4.5	Run practical tests, record gaps, assign owners and keep the plan current.

Involve the people who understand how the business actually operates.

This usually includes the owner or general manager, operations, finance, technology support, people or health and safety, supplier or procurement contacts, and staff who run critical business processes day to day.

Plan overview and control

Plan overview and control confirms what the plan covers, who owns it, who can approve changes, where the current copy is stored and how it can be accessed during disruption.

It should be completed first and checked whenever people, sites, systems, suppliers or business priorities change.

Ownership, scope and access

A BCP needs a named owner so it stays current and can be activated when required.

The plan owner coordinates inputs, maintains the approved copy, schedules reviews and makes sure key people know where the plan is stored.

A backup owner is just as important because disruptions often occur when the owner or key administrator is unavailable.

Scope explains what the plan covers and what is managed elsewhere.

For a smaller business, one plan may cover the whole business.

For a business with multiple sites, entities or trading channels, the plan may need a short site-specific appendix or separate plan for materially different operations.

Scope element	Decision to record
Legal entities and trading names	Which entities, trading names and business units are covered.
Locations and sites	Which offices, workshops, warehouses, farms, mobile operations or branches are covered.
Products, services or channels	Which products, services, customer groups or channels are included.
Critical physical assets	Which machinery, plant, vehicles, tools, stock, utilities or site assets support critical processes.
Critical technology and data	Which key systems and records support critical business processes.
Emergency response and exclusions	How this plan links to immediate safety arrangements and what specialist matters are managed separately.

Document control and offline/offsite access

Document control avoids confusion during disruption.

Use a clear version number and approval date, record who approved the plan, keep one current approved digital copy in a controlled location, maintain controlled offline/offsite copies for the response team and mark superseded copies clearly.

You should ensure that you keep one controlled digital copy in your business's approved secure online filing location, where important records are normally retained, and one secure offline or offsite copy that the response team can access if email, servers or cloud folders are unavailable. This is because you cannot rely on normal systems being available during a disruption.

The offline copy should include the current plan, key contacts, the immediate checklist, priority records and essential bank or insurance details, while still protecting personal, financial and commercially sensitive information.

Quality check: Could someone find and activate the current plan if the owner is unavailable? Are scope, exclusions, approvals, distribution, storage and offline/offsite access clear and current?

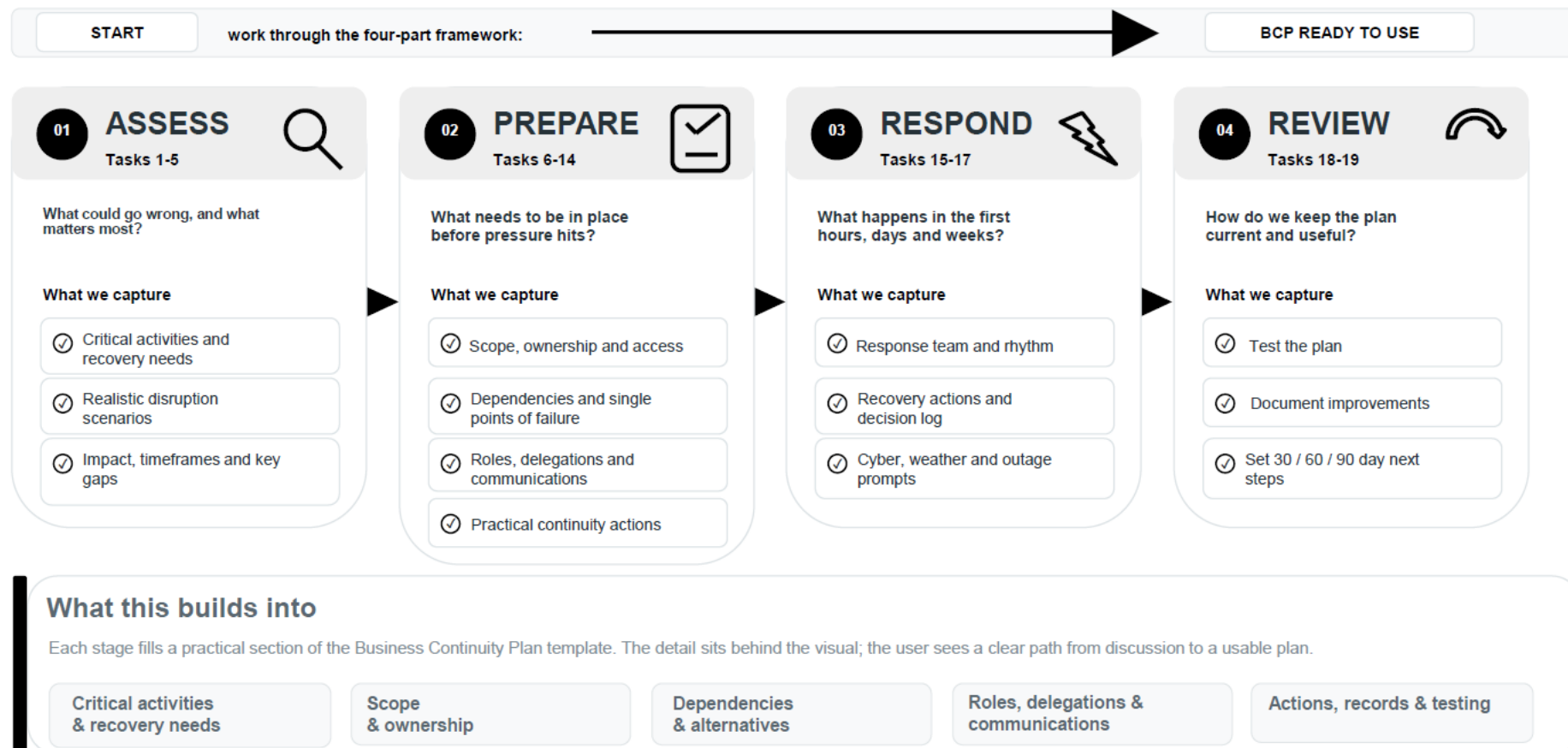
The diagram below shows how the four parts of the Business Continuity Plan framework fit together.

As you work through this guide, each part will be broken down in further detail, starting with Assess, before moving into how to Prepare the plan, respond effectively during a disruption, and reviewing the plan to ensure it remains current, practical and fit for purpose.

Building Your Business Continuity Plan

BUILDING YOUR BUSINESS CONTINUITY PLAN

A simple view of how each section of the process becomes a practical Business Continuity Plan.



1. Assess

Having introduced the framework above, we now turn to the first part of the framework: Assess, which identifies what matters most, what could realistically interrupt it and how quickly disruption becomes a serious problem. The aim is not to create a long risk register. The aim is to identify the business priorities and critical processes that need protection first.

Identify critical business processes

A critical business process is an end-to-end activity that must keep running, or be restored first, to protect people, customers, supply chain, revenue, cash flow, obligations, product or service quality, or reputation.

Start by identifying what the business needs to keep doing during disruption. Focus on practical business outcomes rather than broad labels such as “operations” or “admin”. For example, “run payroll and communicate with staff” is more useful than “HR”, and “complete priority customer orders” is more useful than “sales”.

Describe each process at the right level. A task such as calibrating a machine may be important, but the critical business process may be “manufacture and dispatch priority customer orders”. The plan should focus on the processes that protect the business if normal operations are disrupted.

Keep the initial plan to around five to ten critical business processes. The right processes will vary by industry, operating model, customer commitments, sites, systems, suppliers and regulatory obligations, so you will need to tailor these to your specific business.

Sector process examples

The table below provides examples of critical business processes across different industries to help identify processes at the right level of detail.

Sector	Example outcome / critical process	Why it matters
Retail	Continue essential sales and payment options.	Protects daily revenue and customer access.
Trades / construction	Attend urgent jobs safely.	Protects people, contractual commitments and reputation.
Hospitality	Serve safely at a reduced level or pause safely.	Protects customers, food safety and brand trust.
Professional services	Meet urgent filing and client deadline commitments.	Protects client obligations and reputation.
Manufacturing	Complete priority customer orders and maintain quality checks.	Protects revenue, contractual commitments and future orders.
Primary / agriculture	Maintain animal welfare, water, feed and cold chain.	Protects welfare, product quality and obligations.

Business process examples

The table below provides examples of common processes and what they help to protect.

Use it as a prompt to identify your critical business processes.

Common process	What it protects or unlocks
Take and confirm priority customer orders	Customer commitments, revenue and production priorities.
Plan production and allocate capacity	Use of labour, machinery, materials and time-sensitive work.
Source raw materials	Continuity of raw materials and approved alternatives.
Operate critical machinery or production line	Core product supply and output capacity.
Complete quality checks and release product	Safety, compliance, customer trust and traceability.
Invoice customers and collect cash	Cash flow and funding conversations.
Run payroll and staff communication	Staff trust, availability and welfare.
Maintain records, systems and data access	Job history, pricing, quality records and decision evidence.

Common mistake: Avoid broad entries such as “operations”, “admin” or “finance” on their own. A useful critical process describes the activity that needs to continue or recover, such as “invoice customers and collect cash” or “run payroll and communicate with staff”.

Identify and map supporting functions for critical business processes

Once the critical business processes have been identified, the next step is to identify the functions that support those processes.

Supporting functions are the parts of the business that enable a critical process to operate. These are not separate critical processes on their own.

They help identify who and what each critical process relies on, and where disruption could affect the process. We define those functional areas as people, customer, financial, operational, supply chain and technology (what we refer to as a business’s functions).

Once the supporting functions of a critical business process have been identified, the next step is to map these.

Mapping supporting functions helps confirm whether the business has identified the right critical processes and whether any important dependencies have been missed.

The table below is an example of how different parts of the business are involved in each critical process.

This is not intended to create a complex organisation chart. It is a practical way to confirm who leads the process, who supports it, which functions it depends on, and who may be affected if the process is disrupted.

Tailor this to your specific business.

Critical process - business functions involved

Critical process	People	Customer	Financial	Operational	Supply chain	Technology
Source raw materials	Trained staff backups to manage materials.	Late or poor materials can delay customer orders.	Urgent freight, storage, waste, or replacement materials can increase costs.	Production stops if materials are late, unavailable, or not approved.	Check timing, backup suppliers, and alternative materials.	Some may need manual updates.
Operate critical machinery / production line	Staff cover needed; fatigue risk increases if the issue continues.	Delayed orders, complaints, and new delivery dates.	Extra costs from lost sales, overtime, repairs, idle staff.	Backlog grows when production slows; quality risk increases.	Check spare parts, technicians, and key supplier timing.	Production plans and machine data; use a manual plan if systems fail.
Complete quality checks and release product	Need drivers, dispatch staff, and equipment cover.	Late deliveries can damage customer trust.	Extra courier, freight, and penalty costs may increase dispatch costs.	Finished stock builds up and warehouse space gets tight.	Check carrier space, route issues, and booking cut-offs.	Tracking, invoices, and delivery proof may be delayed; use manual proof if needed.

Identify disruption scenarios

After critical processes have been identified and supporting functions have been mapped, identify disruptions that could stop, slow or materially affect those processes or the supporting functions they rely on.

A disruption may affect one critical process, several critical processes, or one or more supporting functions.

For example, a technology outage may affect customer orders, invoicing, payroll and communication, whereas a key person absence may affect decision-making, payroll, banking access or ability to operate specialist machinery.

The purpose of this step is not to create a separate plan for every possible disruption. The purpose is to identify disruptions and understand which critical processes and supporting functions could be impacted.

For each disruption, consider:

- What could realistically happen?
- Which critical processes could be stopped, slowed or reduced?
- Which supporting functions could be impacted?
- Would the disruption impact more than one process?

The table below provides examples of common NZ disruptions.

Use these as prompts to identify disruption scenarios and consider how each could affect your business's priority, ownership and response actions for its identified critical business processes.

Disruption Scenario	Common NZ disruptions	Critical process potentially affected	Supporting functions potentially affected	Examples of Immediate concern
Severe weather, fire, natural disaster or premises access	Flooding, earthquake damage, fire, storm, snow, road closure or unsafe site access.	Site operations, dispatch, customer service, production, staff access and records access.	People, customer, financial, operational, supply chain and technology.	People safety, fire response, site access, utilities, deliveries, stock or customer access.
Cyber or system outage	Cloud system outage, payment issue, internet outage, suspected cyber incident or data access issue.	Orders, customer communication, invoicing, payroll, payment processing, reporting and records access.	Customer, financial, operational, technology and people.	Access to records, payments, privacy, customer service and communication.
Utility, people or supply chain disruption	Power, gas, water, telecommunications, energy or fuel constraints, illness, key person absence, supplier failure or freight delay.	Production, service delivery, dispatch, payroll, customer commitments and cash collection.	People, operational, supply chain, customer, financial and technology.	Delivery capacity, revenue, cash flow, customer commitments and staff wellbeing.
Business-specific scenario	Equipment failure, animal health event, product quality issue, landlord access issue or specialist license issue.	Depends on the specific process affected.	Depends on the specific process affected.	Depends on the critical process affected.

Gather information, assess impact and likelihood, prioritise risk and determine recovery timeframes

This section brings together the critical processes identified, the supporting functions, and the disruptions identified.

The aim is to make an informed assessment of impact and likelihood. If the business does not gather relevant information before assessing impact, it may underestimate the consequences of disruption, overstate its ability to recover, or prioritise the wrong risks.

Gather information before assessing impact

Before scoring impact or likelihood, gather enough information to understand how disruption could affect each critical process and its supporting functions.

The information gathered should be practical and evidence based. Recent tests, current contracts, supplier confirmations, system backup evidence, staff coverage, access rights, bank authorities and customer commitments are more useful than assumptions.

The table below includes the six functional areas and examples of what to consider and the information that should be gathered to accurately assess impact. Use these as prompts but tailor them to your specific business.

Business area	What to consider	Information to gather to help assess the impact
People	Safety, wellbeing, availability, workload, key person risk and ability to work safely.	Roster, staff contact list, role coverage, safety procedures and wellbeing support.
Customer	Delays, missed promises, complaints, refunds, lost trust or customers going elsewhere.	Customer list, contracts, service promises, complaint history and priority orders.
Financial	Sales or fees stopping, extra costs, working capital pressure, penalties, excesses or lender pressure.	Cash flow forecast, debtors, creditors, payroll cycle, facility limits and cost estimates.
Operational	Backlog, missed deadlines, rework, production constraints, quality issues or reduced capacity.	Job schedule, production plan, order volumes, quality records and delivery deadlines.
Supply chain	Supplier delays, shortages, transport disruption, stockouts, damaged goods or limited alternatives.	Supplier list, lead times, inventory, contracts, freight contacts and substitute options.
Technology	Systems, devices, data, internet, payments, invoicing, cyber risk or manual processing delays.	System list, provider contacts, backup evidence, access rights and offline reports.

Assess impact and likelihood

Once the relevant information has been gathered, assess the impact and likelihood of each disruption affecting each critical process and its supporting functions.

Not all disruptions affect processes in the same way.

A freight delay may have a critical impact on dispatch but only a minor impact on payroll.

A system outage may have a critical impact on invoicing and customer communication but a lower impact on physical site operations.

The assessment should therefore consider the specific combination of:

- the critical process;
- the supporting functions involved;
- the disruption scenario;
- the information gathered; and
- the likely business consequence.

Use the rating guide below.

Each business should tailor the rating definitions to its size, industry, customers, sites, machinery, obligations and risk appetite.

Rating	Impact means	Likelihood means
1 - Low / Unlikely	Minor disruption is manageable through normal processes.	Limited or no likelihood of occurring based on current controls, exposure and dependencies.
2 - Medium / Possible	Noticeable disruption requiring management attention.	Possible likelihood due to some dependencies, known issues or limited alternatives.
3 - High / Likely	Significant disruption to operations, customers, cash flow or obligations.	Likely to occur in some circumstances due to material dependencies or past issues.
4 - Critical / Almost certain	Essential operations stop or major harm is likely.	Expected to affect the process because exposure is high, vulnerabilities are known or feasible alternatives are limited.

Prepare a risk prioritisation list

After impact and likelihood have been assessed, prepare a risk prioritisation list. This list should identify which critical process and disruption combinations need the most attention and present an order of processes.

The highest priority risks are generally those where:

- the impact on the critical process is high or critical;
- the disruption is likely or has occurred before;
- the process supports people, customers, cash flow, obligations, quality or reputation;
- several supporting functions are affected at once;
- there are limited practical backup options;
- the process unlocks other critical processes; or
- the business would quickly exceed its tolerance for disruption.

This risk prioritisation list should guide what the business prepares first in the next part of the framework: Prepare (Section 2 below). It should not be based on likelihood alone. A low-likelihood disruption may still be a high priority if the impact would be severe and there are limited backup options.

Determine recovery timeframes

Once the business has assessed impact, likelihood and risk priority, it can then determine appropriate recovery timeframes.

A recovery timeframe is the target time to restore a critical business process to an acceptable level. It does not always mean returning to normal operations. It may mean operating at a safe reduced level, serving priority customers only, using manual processing, shifting work to another site or using a temporary outsourced option.

Recovery timeframes should be based on the impact and likelihood assessment, not guesswork.

The timeframe should reflect how quickly disruption becomes unacceptable for people, customers, cash flow, legal obligations, product or service quality, supply chain continuity or reputation.

For each prioritised critical process, record:

- the minimum operating level;
- the recovery timeframe;
- the supporting functions needed to recover the process;
- the key assumptions relied on; and
- the information or evidence used to support the decision.

The recovery timeframe should align with the risk prioritisation list.

The highest-priority critical processes generally have the shortest recovery timeframes or the strongest backup arrangements. Lower-priority processes may be able to wait, provided the business has considered the impact of delay.

The below table provides examples of recovery timetables, when to use them and the minimum service level.

Recovery timeframe	Use when	Example minimum service level
Immediate / same day	Safety, urgent customer needs, essential trading, animal welfare or urgent communication.	Confirm staff safety, respond to urgent customers and protect critical records.
1-2 days	Backlog, cost or customer pressure builds quickly.	Operate priority process at reduced capacity with manual or backup action.
3-5 days	Can pause briefly but creates cash, customer or obligation pressure.	Complete only priority orders or obligations.
1-2 weeks	Manageable with reduced goods/services, manual actions or lower-priority recovery.	Defer non-critical work and clear backlog progressively.
More than 2 weeks	Lower-priority tasks that can be deferred safely.	Resume once critical operations stabilise.

Assess summary

By the end of Assess, the business should have:

- Identified the critical business processes that must continue or recover first,
- Mapped the supporting functions that enable those processes,
- Identified realistic disruptions,
- Gathered the information needed to assess impact,
- Assessed impact and likelihood,
- Prepared a risk prioritisation list and
- Determined recovery timeframes for priority processes.

Quality check: Have the most important critical processes been listed in priority order? Have recovery timeframes, acceptable data loss and minimum service levels been recorded? Are disruptions linked to specific processes?

2. Prepare

Building on the critical processes, impact and recovery timeframes identified in Assess, part 2 of the framework focuses on preparing the plan by turning the assessment into practical actions that can be used before pressure hits.

It confirms who will act, what resources are needed, what alternatives are realistic, how communication will work and how the response will scale as facts change.

Roles, contacts and delegated authority

Ownership defines who keeps the plan current and who can activate it. Responsibilities should be attached to roles as well as names, because people move roles or become unavailable. Every important role should have a backup.

Role	Main responsibility	Delegation or access to confirm
Plan owner	Maintains the plan and coordinates reviews.	Authority to update the current copy and schedule reviews.
Response lead	Activates the plan, sets priorities and chairs short check-ins.	Authority to activate the plan and approve urgent priorities.
People lead	Checks staff safety, wellbeing and availability and sends internal updates.	Staff contact access and welfare escalation process.
Operations lead	Confirms affected processes, suppliers, facilities and practical actions.	Authority to prioritise work, switch suppliers or use backup processes.
Technology lead	Checks systems, data, cyber risks and provider escalation.	Provider authority, administrator contacts and escalation process.
Finance lead	Monitors cash, payments, payroll, insurance, funding and evidence.	Banking access, emergency spend authority and broker/funder contacts.
Communications lead	Prepares staff, customer and supplier messages and keeps updates consistent.	Approval process for external messages and contact lists.

Common mistake: Do not assume the owner will always be available or able to lead the response. People manage disruption and stress differently, so name backups, confirm authority limits and give key role holders enough practice.

Dependencies, single points of failure and readiness gaps

A dependency is something the business relies on to keep a critical process running.

A single point of failure is a dependency with no practical backup.

These are often the fastest and most valuable readiness improvements for small and medium-sized businesses.

Dependency type	Questions to ask	Example single point of failure
People / skills	Who can perform the task, approve decisions and access key information?	Only one person can run payroll or operate the machine.
Systems / data	Which systems, records, devices and access rights are needed?	Customer orders are only in one cloud system with no offline export.
Premises / equipment	Which site, plant, vehicles, tools, utilities or stock are essential?	One machine has no spare part or repair arrangement.
Suppliers / logistics	Which suppliers, outsourced providers, routes or lead times matter most?	One freight provider handles all priority deliveries.
Information / records	Which instructions, contracts, quality records, passwords or authorities are needed?	Banking authorities and key contacts are known only by the owner.
Finance / access	Who can approve payments, use bank access and track costs?	Only the owner holds the bank token or emergency spend authority.

When preparing the plan for implementation, compare the business's current readiness with the readiness it needs to maintain minimum operating levels during disruption identified in the assessments completed above.

The difference between current readiness and desired readiness is the readiness gap.

Use evidence rather than optimism: recent tests, named owners, confirmed provider contacts, available spare parts, approved alternates, access rights and records that can be restored or recreated.

Readiness rating	What it means	Evidence to look for
1 - Unknown	Not assessed or no clear proof.	No test, owner or documented practical action.
2 - Weak	Some ability, but unreliable.	Gaps in people, systems, suppliers, plant, equipment, physical assets or authority.
3 - Partial	Basic plan exists, but not fully proven.	Some tests or practical actions documented.
4 - Strong	Practical, tested and owned.	Recent test, clear owner and fallback.

People, safety and wellbeing

People are the first priority. Continuity decisions should not ask staff to work unsafely or ignore fatigue, stress, caring responsibilities, transport disruption or accessibility needs.

The BCP should connect to the Emergency Response Plan and then support the transition to safe continuity operations.

Area	What to plan	What good looks like
Safety check	How staff, contractors and visitors will be accounted for.	Primary and backup contact channels; status recorded as safe, needs help, unreachable or unavailable.
Availability and rosters	How remote work, shifts, fatigue and caring responsibilities will be managed.	Managers know the minimum staff required for each critical process.
Key person backup	Who can cover owner, payroll, banking, operations, systems and customer roles.	Backup named and trained for each critical task.
Wellbeing support	How workload, stress and follow-up support will be handled.	Follow-up rhythm, escalation points and workload limits are clear.
Accessibility support	Support for disabled staff, customers or visitors during emergency and recovery.	Needs considered in safety checks, communications and access arrangements.

Premises, equipment and physical assets

Physical disruption can affect premises access, machinery, plant, equipment, stock, vehicles, utilities, security and site safety.

The plan should turn physical disruption into practical choices: where people will work, which assets are needed first, who can access key locations, whether work can be outsourced or shifted, and what evidence is needed for recovery or insurance purposes.

Confirm alternative work locations or safe remote work options.

Identify essential equipment, plant, machinery, tools, vehicles, stock, utilities and spare parts.

Decide whether production or service delivery can be paused, shifted, outsourced or prioritised.

Record keyholders, alarm codes, landlord contacts, service providers and site access requirements.

Protect premises, stock, equipment and confidential information, and retain evidence such as photos, videos, repair reports and supplier notices.

This is an optional register (Appendix C) in the BCP full template.

Technology, systems, data and manual controls

Technology disruptions are business disruptions. The plan should identify which systems and data support critical processes and how the business will continue safely if they are unavailable. Cloud systems can still be unavailable, inaccessible or affected by incorrect data, so confirm backup access, provider contacts, offline reports, manual actions and reconciliation steps.

Area	What to decide	Example
Key systems	Which systems are needed first for customers, payroll, jobs, supply, payments and records.	Job management, accounting, payroll, customer records, email and phones.
Backups and access	Whether backups, exports or offline access are available and tested.	Daily job schedule export retained securely for priority production.
Manual actions	What can continue manually and where records will be captured.	Manual job records, numbered dispatch records, offline payment process, and daily finance review.
Acceptable data loss	How much information could be lost or recreated.	Same-day job changes must be recreated from manual records and customer confirmations.
Provider escalation	Who contacts providers and who can authorise support.	Technology lead and backup have provider authority and contact details.

Manual actions can keep work moving, but they increase risk. Common risks include lost records, duplicate transactions, pricing errors, privacy breaches, unapproved spend, payroll errors, tax errors and customer confusion. Each manual action needs a simple control.

Manual action	Main risk	Minimum control
Manual order or job record	Pricing errors, duplicate orders or lost records.	Use numbered forms or controlled file, daily approval and reconciliation to the system.
Offline payroll input	Incorrect pay or privacy breach.	Two-person review, secure storage and approved adjustments loaded once systems return.
Manual invoicing	Revenue leakage, tax errors or duplication.	Finance approval, document register and ledger reconciliation.
Alternate supplier ordering	Quality, cost or contract risk.	Approved supplier list, emergency approval and post-event review.
Manual customer updates	Mixed messages or outdated commitments.	Approved message, communication record and next update time.

Practical decision: Do not rely on memory to enter records later. Decide where manual records are kept, who approves them, when they are entered into the system and who reviews exceptions.

Key parties and critical providers

A business can have a strong internal plan but still fail to recover if critical suppliers, outsourced providers, logistics partners, raw material sources or customer expectations are not considered. Identify the value chain arrangements needed to maintain minimum operating levels.

Question	Why it matters	Example practical action
Which suppliers would stop a critical process if unavailable?	Shows where supplier concentration creates a single point of failure.	Pre-approve alternate supplier or substitute material.
What lead times, order limits or quality checks apply?	Avoids unrealistic backup assumptions.	Confirm emergency order limits and quality approval process.
Which customers need priority contact?	Protects trust and contractual commitments.	Name communication owner for top customer groups.
Which outsourced providers support critical work?	Payroll, technology, warehousing or logistics may be outside the business but still critical.	Confirm escalation contact and provider continuity arrangements.

Financial, insurance, obligations and evidence

Disruption often becomes a commercial issue quickly. Once immediate safety and urgent operations are stabilised, the business needs to protect cash flow, pay staff where possible, manage urgent costs, preserve claim evidence, keep obligations visible and communicate with funders or insurers when required.

Area	What to prepare	Why it matters
Cash flow forecast	Current forecast, expected receipts/payments, minimum cash buffer and disruption scenario.	Supports decisions on reduced service, emergency spend and funding conversations.
Banking and funding access	Bank contacts, facilities, tokens, backup approvers and covenant points.	Avoids delay if the owner or normal approver is unavailable.
Payroll	Manual or alternate payroll process, deadlines and approvals.	Protects staff trust and helps maintain continuity.
Insurance	Broker/insurer contacts, policies, claim steps and evidence needs.	Supports timely notification and well-documented claims.
Obligations	Contracts, leases, privacy, employment, tax, health and safety and sector requirements.	Keeps obligations visible and prompts specialist advice where needed.
Cost and loss tracking	Incremental costs, lost revenue, mitigation actions and evidence storage.	Supports insurance, funding, stakeholder and governance records.

Keep evidence organised from the start of the disruption. Insurance and funding discussions often require evidence. Record decisions, costs, losses, photos, videos, repair reports, supplier notices, customer impacts and mitigation actions. Seek guidance from the insurer, broker or adviser before committing major recovery spend where practical.

The BCP should identify obligations and decision points. It should not replace specialist legal, tax, insurance, employment, cyber security, health and safety, financial or sector-specific advice.

Communication plan and message templates

Communication should be planned before disruption. The first message does not need every answer. It should be factual, clear and consistent: what is known, what is being done, what changes for the audience and when the next update will come.

Audience	Need to know	Typical owner
Staff and contractors	Safety, work arrangements, expectations, support and next update time.	People lead / communications lead.
Customers	Service changes, delays, alternatives, priority handling and next update time.	Customer lead / communications lead.
Suppliers and logistics providers	Changed demand, delivery priorities, constraints, payment or timing changes.	Operations lead.
Funders and insurers	Impact, evidence, cash flow, claim or funding steps.	Finance lead.
Landlords, regulators or advisers	Access, compliance, lease, licence or specialist advice matters where relevant.	Response lead / relevant adviser.
Media or community	Simple public message where relevant and approved.	Named spokesperson only.

Message templates prepared in advance save time and reduce the risk of inconsistent or speculative communication. Keep templates short and factual. Avoid blaming suppliers, naming cyber as the cause before it is confirmed, promising recovery times that are not yet reliable, or sharing sensitive information.

Example customer holding message: We are currently managing a disruption affecting [service or order type]. We are prioritising urgent commitments and will update you by [time/date]. For urgent matters, contact [details].

Prepare quality check: Have single points of failure been identified? Are practical actions owned, realistic and tested or scheduled for testing? Are response roles, backups and delegated authority clear? Are communication owners, channels and next update timings documented? Are manual action controls and evidence requirements ready?

3. Respond

Respond is where the plan is used during disruption. The aim is to protect people, establish facts, activate the response team, make clear decisions, communicate early, record evidence, start practical actions and manage recovery. The plan should remain adaptable because facts, risks and priorities may change.

Activation triggers and escalation thresholds

Activation triggers help the business decide when to move from normal management to a coordinated BCP response and which escalation level applies. Triggers should be practical and observable. If there is immediate danger, follow the Emergency Response Plan first and call emergency services where required.

Trigger type	Example threshold	Initial action
People safety risk	Injury, evacuation, significant welfare concern or unsafe work condition.	Follow emergency response, account for people and activate people lead.
Loss of site or premises access	Site unavailable or unsafe beyond the agreed tolerance or threshold.	Assess remote, alternate-site or temporary closure arrangements.
Critical system outage	Priority system unavailable beyond agreed timeframe or integrity uncertain.	Pause risky activity, contact support and activate manual actions if safe.
Supplier or logistics disruption	Critical supplier cannot meet delivery or freight route unavailable.	Confirm impact, alternatives and customer priority.
Customer, revenue or cash impact	Material delay, lost revenue, cash pressure or priority customer impact.	Prioritise service, cash and stakeholder communication.
Privacy, legal, regulator or media risk	Potential notifiable issue, public attention or regulator contact.	Centralise communication and seek appropriate advice.

Not every disruption requires full activation straight away. Some events develop as facts change, such as a heavy rain warning becoming a site leak, then a river breach threatening major flooding. For high or critical scenarios, define simple escalation levels.

Level	Use when	Response focus
Level 1 - Monitor and prepare	A warning sign exists, but critical processes are still operating.	Check people, site, suppliers, customer commitments, evidence needs and communication drafts.
Level 2 - Partial activation	One or more critical processes, sites, suppliers, customer groups or cash flow assumptions are under pressure.	Activate relevant roles, protect stock/records, move priority work and contact affected stakeholders.
Level 3 - Full activation	Critical processes are materially disrupted or there is significant people, financial, legal, privacy, media or reputational risk.	Activate the response team, start simple decision and action records, use recovery action plans, issue situation updates and preserve evidence.
Level 4 - Recovery and stand-down	The immediate disruption is stabilising.	Manage backlog, reconcile manual records, confirm stakeholder updates, capture costs/evidence and complete return-to-normal.

Immediate response checklist

The immediate response checklist should be short enough to use under pressure. It should guide the first actions, not replace judgement.

The first priority is always life safety and immediate hazards.

Consider what needs to happen as soon as an incident happens, including:

1. Confirm life safety, emergency services involvement and immediate hazards.
2. Open a simple incident record and capture known facts, times, sources and first decisions.
3. Confirm affected people, sites, systems, suppliers, customers, data and cash flow.
4. Decide whether to activate the plan and name the response lead and backups.
5. Agree immediate priorities, meeting rhythm and next update time.
6. Issue the first staff message with safety instructions and next update time.
7. Preserve evidence for insurance, legal, privacy, cyber security or funding purposes.
8. Start approved practical actions for priority processes.

First hour, first day and first week

Use the response rhythm to keep the response practical and focused.

Short, regular check-ins are usually more useful than long meetings during uncertainty.

Timeframe	Focus	Typical actions
First hour	Safety, control and clarity.	Check people are safe; establish facts; activate response lead; agree roles, decision rights and update cadence; protect evidence.
First day	Stabilise priority activities.	Assess impact on critical processes; start practical actions; send holding messages; confirm customer, supplier and cash priorities; record decisions.
First week	Recover, manage backlog and learn.	Stabilise operations; manage fatigue and capacity; track costs and risks; review stakeholder expectations; capture lessons and update the plan.

Decision rights, records and recovery actions

Decision rights are the disruption-specific delegation of authority. During disruption, the business may need to approve urgent spend, pause activity, prioritise customers, notify insurers, change supplier arrangements or approve external statements. Identify who has authority to make these decisions, their backup and what evidence is required.

Decision / authority	Authority / evidence to record
Activate or stand down the plan.	Date/time, trigger, decision-maker and reason.
Approve emergency spend.	Amount, reason, quote or invoice, approval and expected recovery benefit.
Prioritise customers or services.	Criteria used, customers affected and communication record.
Pause unsafe system activity.	Technology advice, time paused, systems affected and restart criteria.
Notify bank, insurer, regulator, landlord or adviser.	Trigger, message sent, recipient, time and response received.
Approve external message.	Approved wording, audience, channel, sender and next update time.

A simple incident record captures what was decided, by whom, why and what happens next. The recovery action plan turns decisions into owned actions.

A communication record captures what was communicated, when, to whom and by whom. These records support accountability, reduce rework and may assist later insurance, funding, customer, governance or adviser discussions.

Weak action	Stronger action
Look into suppliers.	Operations lead to contact approved backup supplier by 11am, confirm capacity for the priority order batch and record quote in evidence folder.
Update customers.	Communications lead to send approved priority customer update by 3pm and record recipients and next update time.
Fix system issue.	Technology lead to contact provider, confirm outage scope, advise what activity is paused and update response team by 12pm.

Practical decision: It is acceptable to say what is known, what is being checked, what action is required now and when the next update will come. Avoid speculation, blame, unconfirmed causes or unsupported recovery promises.

Scenario response prompts

Scenario prompts help the response team tailor the core plan to the disruption type.

Complete short playbooks only for scenarios rated high or critical in Assess.

Keep them practical and link them back to critical processes, roles and standing backup actions.

Scenario	First response focus	Evidence / control to remember
Cyber or system outage	Pause activity that could increase harm, escalate to the response lead and technology support, and use agreed manual actions for priority work only.	Avoid naming cyber as the cause until confirmed. Record legal, privacy, banking, insurance and customer decision points.
Severe weather or site access issue	Follow official advice and safety requirements first, then check people, site access, utilities, suppliers, customer commitments and remote/alternate-site options.	Keep photos, official notices, supplier notices, customer impacts, costs and decisions.
Key supplier or logistics disruption	Confirm impact, duration, alternate sources, lead times, customer prioritisation and cash flow implications.	Record supplier notices, revised commitments, cost impacts and approval for substitutes or alternate freight.
Critical equipment or physical asset failure	Stop unsafe use, contact maintenance support, confirm spare parts, alternate capacity, outsourcing and quality requirements.	Retain photos, repair reports, quotes, lost production evidence, quality checks and customer updates.
People unavailability or health event	Confirm safety, wellbeing, availability, minimum staffing, rosters and backup decision-makers.	Record staff status, privacy-sensitive information securely and update workload/fatigue decisions.

Situation updates and return to normal

A situation update gives the response team and key stakeholders a concise view of what is happening, what is affected, what decisions are needed and when the next update will come.

It should separate confirmed facts from assumptions and store the update with incident records.

Return to normal should be controlled.

Do not stop continuity arrangements until the business has confirmed which processes are restored, what records need reconciliation, what commitments remain open, what claims or costs need evidence and what lessons should be captured.

- ✓ Critical processes are restored to approved minimum or normal service levels.
- ✓ Manual records have been entered into systems and reconciled.
- ✓ Health, safety and wellbeing risks have been assessed for return to site or normal work.
- ✓ Customer, supplier, insurer, funder, regulator and owner updates have been issued as needed.
- ✓ Incremental costs, losses and claim evidence are stored.
- ✓ Backlog, quality issues and improvement actions are assigned to owners.

Respond quality check:

Could the response team use the plan in the first hour, first day and first week?

Are activation triggers, decision rights and simple records ready?

Are communication owners, channels and next update timings clear?

Are records and evidence captured as decisions are made?

4. Review

Review keeps the BCP current and useful. The best time to find a gap is during a short test, not during a real disruption. Testing does not need to be complex. It needs to be regular, practical and acted on.

Practical tests

Use practical tests to validate whether the plan can be used under pressure.

Record what was tested, what worked, what gaps were found and who owns the improvements. Use the same testing record for planned tests, real disruptions and near misses.

The table below provides common examples of practical BCP tests, what they typically check, and the types of issues they may uncover.

Test	What to check	Example issue found
Contact test	Response team, critical staff and key external contacts can be reached using planned channels.	Backup person not aware of role or contact details out of date.
Manual action drill	One order, job, invoice, payroll input, dispatch record or production run can be processed manually.	No clear numbering, approval, secure storage or reconciliation step.
Backup and document access check	Plan, key contacts, critical records, system backups, bank facilities and insurance policies can be accessed outside normal systems.	A backup exists but cannot be restored or accessed by the right person.
Supplier, bank and facilities check-in	Contacts, lead times, order limits, facilities, claim steps and access arrangements remain current.	Relationship manager, landlord contact or key supplier terms have changed.
Scenario simulation	The response team can work through a realistic high or critical scenario using roles, decisions, communications and recovery actions.	Escalation thresholds, authority limits or customer priority rules are unclear.

After-action review and improvement actions

Complete an after-action review after a real disruption, near miss or meaningful test. The purpose is learning and improvement, not blame. Record lessons while they are fresh and convert them into owned improvement actions.

- What happened and what was the timeline?
- Were people safe, contacted and supported?
- Which critical processes were disrupted and were recovery timeframes met?
- Did practical actions and manual controls work?
- Did communications work as intended?
- Were decisions, costs, losses and evidence recorded?
- What should change in the plan, training, contracts, systems or controls?

Maintenance cycle and review triggers

The plan owner should maintain a simple rhythm for review. During the build, review open actions monthly.

Once the plan is established, check contacts, roles and critical suppliers quarterly, review the full plan every 6-12 months, run a scenario test at least annually, and update the plan after material changes, tests or disruptions.

Trigger	What to update
People or role change	Owners, backups, staff contacts, delegated authorities and critical task cover.
Supplier or customer change	Critical suppliers, priority customers, lead times, service promises and contact details.
System or site change	Software, access, backups, alternate locations, equipment, utilities and support contacts.
Insurance, bank or contract change	Policy details, facilities, covenants, contractual obligations and evidence.
After a disruption or test	What worked, what did not, decisions, lessons and improvement actions.
Regular review cycle	Contacts, roles, suppliers, systems, backups, assumptions and actions.

30 / 60 / 90 day roadmap and readiness checklist

The 30 / 60 / 90 day roadmap, shown below, is a suggested approach to developing and implementing your business's BCP.

Tailor the timing to the size, complexity and risk profile of your specific business.

Timing	Recommended focus
30 days	Confirm plan owner and backup, complete critical process register, populate contacts and response roles, agree quick-win actions.
60 days	Complete business impact assessment and dependencies, document practical actions, draft communications and response checklists, close critical readiness gaps.
90 days	Run a simulation, test contact lists, backups and manual actions, update the plan from lessons and approve the review cycle.
Ongoing	Monthly action review during build, quarterly continuity review, annual scenario test and immediate update after incidents or material change.

Before approval, check the following are complete enough to use.

- Ownership
- Scope,
- Contacts,
- Critical processes,
- Recovery timeframes,
- Single points of failure,
- Practical actions,
- Communication arrangements,
- Evidence requirements,
- Activation triggers
- Review cycle.

Evidence matters: a tick without evidence is less useful than a clear action with an owner and date.

Review quality check:

Has the plan been tested or scheduled for testing?

Is there a review owner and next review date?

Are contact tests, manual action drills and backup/document access checks recorded?

Are lessons converted into improvement actions with owners and due dates?

Quick references

These quick references replace the longer appendices in the previous version.

Keep detailed examples, optional contact lists and site or equipment recovery registers in the BCP template or a separate supporting pack, rather than in the main guide.

Guide-to-template map

Guide part	Template section to complete	What to record
Plan overview and control	Plan overview and control	Ownership, scope, current approved copy, offline/offsite access, version control and next review.
1. Assess	1.1A, 1.1B, 1.1C, 1.2 and 1.3	Critical process priority, function and dependency impacts, recovery needs, minimum service levels, data loss limits, realistic scenarios, ratings and practical responses.
2. Prepare	2.1 to 2.7 and appendix C where relevant	Owners, backups, contacts, dependencies, readiness gaps, practical actions, communications and evidence arrangements.
3. Respond	3.1 to 3.8	Incident-use triggers, checklists, decision records, actions, communications, updates and controlled return-to-normal steps.
4. Review	4.1 to 4.5	Testing, lessons, improvement actions, maintenance rhythm and approval readiness.
Optional supporting detail	Template Appendix B and Appendix C where relevant	Detailed contacts and site, asset or equipment recovery detail that would otherwise clutter the main plan.

Quick glossary

Term	Meaning
Business Continuity Plan (BCP)	A practical plan for keeping the business operating and recovering after an unplanned disruption.
Emergency Response Plan (ERP)	The immediate safety plan for evacuation, first aid, site control and urgent life-safety actions.
Critical business process	A process that must keep running or be restored first to protect people, customers, cash flow, obligations or reputation.
Recovery timeframe	The target time to restore a critical process to an acceptable level.
Minimum operating level	The lowest acceptable service or product supply that can be provided safely during disruption.
Acceptable data loss	The amount, age or sensitivity of information the business could afford to lose or recreate.
Practical action / backup action	The agreed action to keep a critical process moving when normal resources are unavailable.
Situation update	A short, structured update on current impact, actions, decisions and next steps.

Notes:

