

Business Continuity Checklist

A checklist to build and maintain a business continuity plan.

Assess risks and impact

- List the threats most likely to disrupt your business.
- Assess the likelihood and impact of each threat.
- Estimate how long you could survive without key operations.
- Identify single points of failure in your business.
- Note dependencies on suppliers, systems and key people.
- Prioritize the risks that need a plan first.

Identify critical functions

- List the functions that must keep running to serve customers.
- Set a recovery time objective for each critical function.
- Identify the people, systems and data each function needs.
- Cross-train staff so no function relies on one person.
- Document the minimum resources needed to operate.
- Rank functions so you know what to restore first.

Protect data and backups

- Identify the data and records you cannot afford to lose.
- Set up automatic backups on a regular schedule.
- Store backups offsite or in the cloud, separate from your systems.
- Test restoring from a backup to confirm it works.
- Secure systems with strong access controls and updates.
- Keep copies of critical documents and credentials securely.

Plan communication

- Create a contact list for staff, suppliers and key partners.
- Define who decides and who communicates during a crisis.
- Prepare message templates for staff, customers and media.
- Choose backup communication channels if primary ones fail.
- Plan how to keep customers informed of disruptions.
- Store contact and communication plans where they're reachable offline.

Prepare alternatives and recovery

- Identify backup locations or remote work options.
- Line up alternative suppliers for critical inputs.
- Confirm insurance covers relevant disruptions.
Coverage and requirements vary by jurisdiction — confirm with your provider.
- Build a cash reserve or access to emergency funds.
- Document step-by-step recovery procedures.
- Assign clear roles for executing the recovery.

Test and maintain the plan

- Run a tabletop exercise to walk through a scenario.
- Test backups and recovery steps in practice.
- Capture lessons learned and update the plan.
- Train staff so everyone knows their role.
- Review the plan at least once a year.
- Update it after any major change to the business.