



FREE CHECKLIST

Business Continuity Checklist for SMBs

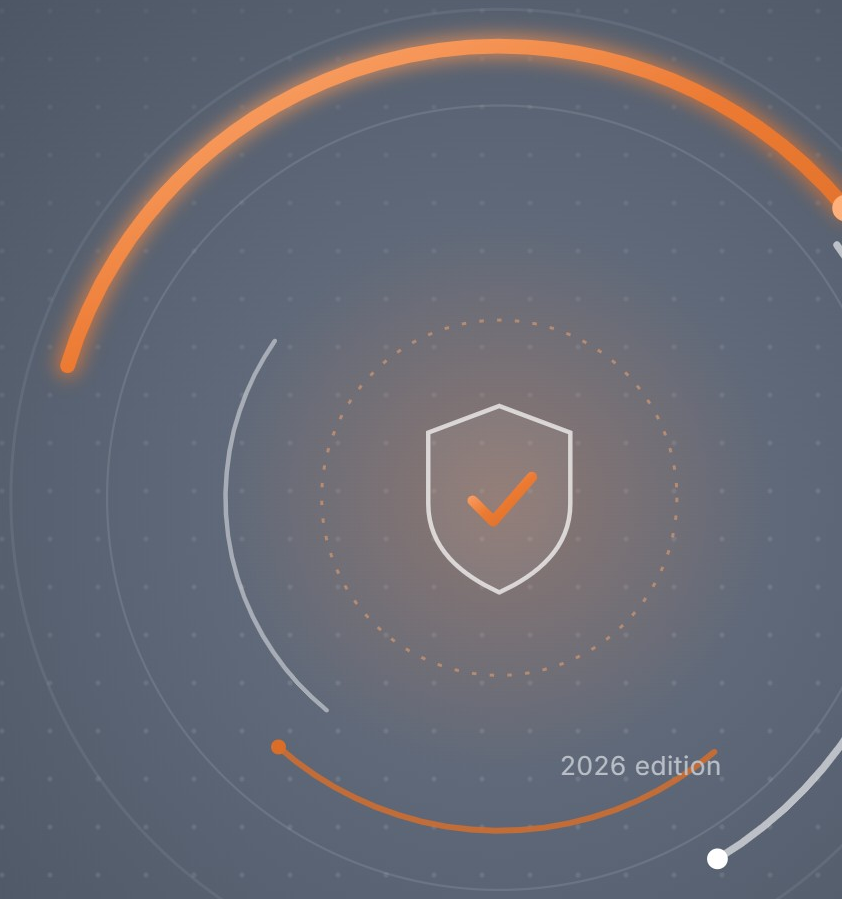
What to have in place so a disruption becomes a bad day, not a business-ending week.

INSIDE

8 areas to check · a fill-in critical process table · an incident decision tree · a testing and review calendar

balancelogic.com · 301-396-8455

2026 edition



HOW TO USE THIS CHECKLIST

Every business gets disrupted eventually: a ransomware attack, a failed server, a flooded office, a key vendor going dark. The ones that recover quickly decided ahead of time what matters most and how they'd get it back.

This checklist is for small and mid-sized businesses (SMBs) without a full-time technology executive. Work through it with the people who actually run your business, not only your IT contact. Start with section 1: how fast each part of the business needs to come back. Everything else follows from those answers. Tick what you have, and give each gap an owner and a date.

Tip: a short plan people can find and follow beats a long one nobody has read. Aim for something your office manager could open on a phone during an outage and act on.

1. Business impact analysis

A business impact analysis answers one question: if this stopped working, how much would it hurt, and how quickly? Start with processes (what the business does), then list the systems and people each one needs.

Two terms worth getting right

RTO: Recovery Time Objective

How long a process can be down before the damage becomes serious. If payroll has a 24-hour RTO, you need it running again within a day.

RPO: Recovery Point Objective

How much recent work you can afford to lose. If your client files have a 4-hour RPO, you need a copy no more than 4 hours old at all times.

- ☐ We've listed the processes that keep the business running and earning: serving clients, billing, payroll, ordering, scheduling, and so on.
- ☐ Each critical process has a named owner who can make decisions about it during an outage.
- ☐ For each process, we know which systems, data, people, vendors and locations it depends on.
- ☐ Leadership has agreed an RTO and RPO for each critical process, in plain business terms.
Leadership decides, with your technology owner explaining what each target costs.
- ☐ We've noted a manual workaround for each process, even a basic one (paper forms, phone orders, a spreadsheet).
- ☐ We've ranked processes so everyone knows what gets restored first.
- ☐ We've checked our contracts for promises to clients that a long outage would break.

Critical process worksheet

Fill in one row per critical process. Use hours or days for RTO and RPO. Rank 1 is restored first.

Process	Owner	Systems and data	RTO	RPO	Manual workaround	Rank

Example row: Client billing · Finance manager · Accounting system, client contracts, email · RTO 3 days · RPO 1 day · Invoice from a saved template · Rank 3

2. People and communication

- ☐ A small response team is named, with a lead and a backup for each role.
- ☐ We have an up-to-date contact list for staff, key clients, vendors, our IT provider, our insurer and our bank, stored somewhere that works when our systems don't.
A contact list that lives only on the file server is no help when the file server is down.
- ☐ We have a way to reach staff that doesn't depend on company email, such as a text group or a phone tree.
- ☐ Someone is responsible for client communication, with short pre-written messages for common scenarios.
- ☐ We know who may speak to the media, clients and regulators, and everyone else knows to refer questions to them.
- ☐ At least two people can approve emergency spending and sign off on recovery decisions.
- ☐ Critical knowledge isn't held by one person. Key procedures and passwords are documented and stored securely.

3. Technology recovery

Backups

- ☐ Every system and data set on the critical process worksheet is backed up, and backup timing matches its RPO.
- ☐ Restores are tested on a schedule, and we've timed a full restore of at least one critical system against its RTO.
A backup you haven't restored is a hope, not a plan.
- ☐ At least one copy is kept offsite or in a separate cloud account, away from the main systems.
- ☐ At least one copy is immutable, meaning it can't be changed or deleted for a set period, even by an administrator.
Ransomware often targets backups first. An immutable copy is still there when you need it.
- ☐ Backup access uses separate credentials and multi-factor authentication.
- ☐ Someone checks the result of every backup job and follows up on failures.

Cloud applications

- ☐ We know which cloud apps hold critical data: email, file sharing, accounting, CRM, line-of-business software.
- ☐ We've confirmed what each provider backs up, how long they keep deleted data, and how we'd get it back.
Most cloud providers keep the service running. Protecting and restoring your data is often your job.
- ☐ Where the provider's retention isn't enough, we have our own backup of that data.
- ☐ Admin accounts for cloud apps are protected with multi-factor authentication and aren't shared.

Systems and access

- ☐ We have a current list of servers, network equipment, laptops and key software, with license and support details.
- ☐ Recovery steps for each critical system are written down, not held in one person's head.
- ☐ We know how long replacement hardware would take to arrive, and what we'd use in the meantime.
- ☐ Emergency admin access is documented and stored securely offline.

4. Vendors and dependencies

- ☐ We've listed the vendors each critical process depends on: internet, phones, software, payment processing, suppliers, outsourced services.
- ☐ For each critical vendor, we know their support contacts, their service commitments, and how they'd tell us about an outage.
- ☐ We've asked our most important vendors about their own continuity plans, and kept the answers.
- ☐ Where one vendor failing would stop the business, we have an alternative identified, such as a backup internet connection or a second supplier.
- ☐ Contracts say who owns our data and how we'd get it back if a vendor fails or we leave.
- ☐ We know what our cyber and business interruption insurance covers, what it requires us to do, and who to call to file a claim.
Many policies set notification steps and approved responders. Find out before you need them.

5. Facilities and remote work

- ☐ If the office is unavailable, we know where people will work and how they'll get access to systems.
- ☐ Staff who may need to work remotely have a company device, or a secure way to connect from their own.
- ☐ Remote access has been tested with the number of people who'd actually need it at once.
- ☐ Phones can be forwarded to mobiles or another site, and someone knows how to do it.
- ☐ Critical paper records are scanned or stored somewhere protected from fire and water.
- ☐ Equipment rooms have power protection, and we know what happens to the network during a power cut.
- ☐ Emergency procedures for the building (evacuation, utilities, alarm company, landlord contact) are documented.

6. Incident decision tree

When something goes wrong, work down these questions in order. The aim is to make the first hour calm and consistent, whoever happens to be on shift.

1. Is anyone in danger, or is the building unsafe?

Yes: people first. Call emergency services, evacuate, and tell the response lead once everyone is safe.

No: go to question 2.

2. Could this be a cyberattack?

Signs include a ransom message, files that won't open, unexpected password resets, unfamiliar logins, or a client reporting odd emails from you.

Yes or unsure: disconnect affected devices from the network but leave them powered on. Call your IT or security provider and your insurer's incident line. Don't wipe, rebuild or pay anything until they advise. Write down what you saw and when.

No: go to question 3.

3. Will a critical process be down longer than its RTO?

Yes, or you can't tell yet: the response lead declares a continuity event. Start manual workarounds, restore in rank order from the worksheet, and send the first staff and client updates.

No: handle it as a normal support issue, but set a time to check again. Problems often grow.

4. Does it involve client data, regulated data or a contract commitment?

Yes: bring in leadership and, where needed, legal counsel and your insurer to decide on notifications. Many contracts and regulations set reporting deadlines.

No: continue recovery and keep a simple log of actions and decisions.

5. Is the business back to normal?

Yes: tell staff and clients, then hold a short review within two weeks: what worked, what didn't, and what to change in the plan.

No: the response lead resets priorities and the next update time, and you keep going.

7. Testing and tabletop exercises

A plan is only as good as the last time someone tried it. Mix these four kinds of test through the year. After each one, record what went wrong, give each fix an owner and a date, and update the plan.

Walkthrough

Owners check that contacts, steps and logins in their section are current.

Tabletop exercise

Leaders talk through a realistic scenario and note where the plan is unclear.

Restore test

IT restores a real system or data set from backup and times it against the RTO.

Live switch

Staff work from the alternate setup for a few hours.

Tabletop scenarios to start with

Ransomware encrypts the file server on a Monday morning. Your main line-of-business software provider is down for two days. Water damage closes the office for a week. A finance staff member wires money after a convincing email from a "client."

8. Review cadence

When	What to review	Done
Quarterly	Contact lists, response team roles, backup results and failures	☐
Twice a year	A restore test of one critical system, plus a walkthrough or tabletop	☐
Once a year	The full plan, RTO/RPO targets, vendor list and insurance cover	☐
After any major change	New system, office move, new key vendor or big staff change	☐
After any real incident	What worked, what didn't, and the fixes to add to the plan	☐

Plan owner: _____ Next full review: _____

Want help turning this checklist into a plan?

Business continuity touches every part of the technology function: systems, vendors, cloud apps, people and budgets. As a Managed Technology Provider, Balancelogic owns that function and makes sure your continuity plan fits how the business actually works.

Book a free IT Strategy Session.

balancelogic.com/contact-us · 301-396-8455 · 3825 Leonardtown Road, Suite 5, Waldorf, MD 20601