CHECKLIST

10 step disaster recovery checklist

A practical, step-by-step checklist for building or reviewing your disaster recovery (DR) plan and a downloadable review plan template

This checklist comes with expert tips from our business continuity specialists, to guide you through disaster recovery planning at every stage.

Work through each section with the appropriate stakeholders to give you an effective, actionable DR plan. Ensuring every action is completed and validated helps to embed a business continuity mindset across the business.

10-step disaster recovery plan checklist:

1. Set clear objectives

Expert tip: Clarity at this stage shapes the direction of your plan and secures business-wide alignment from day one.

	Define the purpose, scope and intended outcomes of the DR plan
	Identify the business priorities the plan must protect (revenue, operations, reputation, compliance)
	Map all applicable regulatory requirements (e.g. GDPR, industry standards)
	Establish acceptable downtime and data loss thresholds at a high level
	Secure senior leadership approval and sponsorship
	Align DR objectives with the wider business continuity strategy

2. Build a complete view of your entire IT estate

Expert tip: Take a business-first approach, working across departments to understand the true impact of downtime and data loss.

	Create a full inventory of systems, applications, infrastructure and devices
	Document hosting environments (on-premises, cloud, hybrid)
	Classify systems. Define what is business-critical, important, non-essential, and so on
	Identify system interdependencies and possible single points of failure
	Map data flows and key integrations
	Assign a business owner to every critical system
	Have reviewed and validated the inventory within the last 12 months

3. Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)

Expert tip: Review recovery objectives regularly to keep pace with changing business priorities and data value.

	Define RTOs for all systems
	Define RPOs for all systems
	Centralise all RTO/RPO data in a single, controlled register
	Validate targets with business stakeholders, not just the IT department
	Ensure backup frequency aligns with RPO requirements
	Confirm recovery solutions can meet RTO targets
	Have reviewed and updated RTO/RPOs within the last 12 months

4. Prepare your disaster recovery team

Expert tip: Cross-train your team and keep documentation accessible so the plan works even when key individuals are unavailable.

	Define all DR roles, responsibilities and accountabilities
	Assign named individuals and deputies for every role
	Deliver targeted DR training for all responsible staff
	Document escalation routes and decision authority
	Store contact details in both the DR plan and offline copies
	Schedule regular training refresh cycles
	Verify backup personnel can carry out primary roles independently

5. Establish a communication strategy

Expert tip: Pre-approved templates and backup communication methods save critical time during high-pressure incidents.

	Define internal communication methods during incidents
	Define an external communication approach for customers, suppliers and partners
	Create and approve message templates for common scenarios
	Document alternative communication channels if core systems fail
	Assign a communications lead for incidents
	Include out-of-hours contact arrangements
	Define PR and media escalation processes

6. Strengthen prevention and resilience

Expert tip: Combine technology, process and proactive monitoring to reduce both the likelihood and impact of incidents.

	Have reviewed and updated cyber security controls within the last 12 months
	Implement endpoint protection, firewalls and intrusion detection
	Establish patching and vulnerability management processes
	Enable proactive monitoring for performance, uptime and threats
	Assess physical security across all key locations
	Evaluate third-party and supply chain risks
	Have completed a formal cyber security risk assessment within the last 12 months

7. Define incident response procedures

Expert tip: Keep procedures clear, accessible and easy to follow so teams can act quickly under pressure.

	Document step-by-step response procedures for likely incident scenarios
	Cover IT recovery, operational continuity, communications and customer impact
	Define who activates the DR plan and under what conditions
	Include telephony and call rerouting processes
	Ensure procedures are accessible offline and not system-dependent
	Review procedures with all relevant teams
	Confirm all instructions are clear, structured and jargon-free

8. Enable alternative working arrangements

Expert tip: Ensure connectivity, equipment and security controls are ready in advance to maintain productivity anywhere.

	Identify viable alternative workspace options (remote, secondary sites, recovery facilities)
	Secure access to work area recovery facilities where required
	Document activation processes for alternative workspaces
	Implement secure remote access (VPN, cloud platforms, MFA)
	Ensure compliance and data security controls extend to remote working
	Test remote access capability for critical users
	Define workspace and equipment requirements for key teams

9. Validate your disaster recovery environment

Expert tip: Ensure your DR environment can automatically replicate workloads and support rapid, real-time recovery.

	Define and documented the DR site (cloud, colocation or physical)
	Confirm geographic separation from the primary environment
	Test failover from primary to DR site
	Verify data replication meets RPO requirements
	Document failback procedures to the primary site
	Review SLAs and support arrangements with providers
	Confirm DR capacity can handle peak operational demand

10. Test, review and continuously improve

Expert tip: Regular testing is critical, it's the only way to prove your plan works and identify gaps before a real incident.

	Have completed a full DR test or simulation within the last 12 months
	Record outcomes, gaps and lessons learned
	Remediate all critical issues identified during testing
	Schedule the next DR test with a fixed date
	Review the plan after major changes, incidents or acquisitions
	Store the DR plan securely with an accessible offline copy
	Secure annual senior leadership review and approval

Disaster recovery plan review log

Track changes, maintain accuracy and ensure continuous improvement.

Use this log to record all reviews, updates and approvals. This provides a clear audit trail and helps demonstrate compliance, accountability and continuous improvement.

How to use this log

- Record every formal review, update or test of you DR plan
- Capture both planned reviews and updates triggered by incidents or changes
- Ensure each entry is signed off by an authorised reviewer
- Keep this log stored with both digital and offline copies of your plan

Version	Date	Reviewed By	Change Type	Summary of Changes	Trigger (An-nual Review / Test / Inci-dent / Change)	Approved By	Next Review Date