

Business Continuity & Disaster Recovery Checklist

A concise review for SMEs that need to understand whether important services can be recovered within a business-acceptable timeframe.

Business priorities

☐	Critical business services and their owners are documented.	Yes / Partly / No
☐	Recovery Time Objectives are agreed with business stakeholders.	Yes / Partly / No
☐	Recovery Point Objectives reflect acceptable data loss.	Yes / Partly / No
☐	People, premises, technology and supplier dependencies are mapped.	Yes / Partly / No
☐	Manual workarounds are documented for the highest-priority processes.	Yes / Partly / No

Backup design

☐	Backups cover servers, cloud services, applications and configuration where needed.	Yes / Partly / No
☐	At least one backup copy is isolated from normal administrator access.	Yes / Partly / No
☐	Backup retention supports business, contractual and regulatory needs.	Yes / Partly / No
☐	Backup failures generate alerts that are owned and investigated.	Yes / Partly / No
☐	Encryption keys and recovery credentials are protected and recoverable.	Yes / Partly / No

Recovery capability

☐	Restore tests are performed and evidenced at an agreed frequency.	Yes / Partly / No
☐	Identity, DNS, networking, certificates and integrations are included in recovery plans.	Yes / Partly / No
☐	Alternative communications are available if normal systems fail.	Yes / Partly / No
☐	Key suppliers and escalation contacts are recorded outside primary systems.	Yes / Partly / No
☐	Recovery documentation is accessible during a major outage.	Yes / Partly / No

Exercises and improvement

☐	A named person can declare a technology incident or disaster.	Yes / Partly / No
☐	Scenario exercises include cyberattack, supplier outage and site loss.	Yes / Partly / No
☐	Exercise actions have owners and completion dates.	Yes / Partly / No
☐	Material technology changes trigger a continuity-impact review.	Yes / Partly / No
☐	Senior management reviews resilience risks and unresolved recovery gaps.	Yes / Partly / No

Priority actions

1. _____
2. _____
3. _____

This checklist is general guidance, not legal, regulatory or security assurance. The appropriate controls depend on your organisation, risks, contracts and regulatory obligations.