

Business Backup & Recovery Checklist

A practical checklist to help your business review its backup configuration, recovery procedures and protection against data loss.



A backup is only useful if you can restore from it when you need to. Use this checklist to review what you back up, where it goes, how it is protected and whether recovery has actually been tested.

Business name

Review date

Reviewer

Next review due

A 'backup successful' message is not proof you can recover

Backup software can report success while files are missing, corrupted, encrypted by ransomware or impossible to restore in time. The only reliable evidence is a **restoration test**: actually restoring data and checking that it opens and is complete.

Two terms worth understanding

Term	In plain English	Example
Recovery time objective (RTO)	How long your business can cope without a system before the disruption becomes serious. It is your target time to get back up and running.	Accounts must be working again within 1 business day.
Recovery point objective (RPO)	How much recent work you could afford to lose, measured in time. It decides how often you need to back up.	Losing more than 4 hours of email would be unacceptable, so back up at least every 4 hours.

What needs protecting

Done	Item
☐	Critical business data is identified Customer records, financial data, contracts, designs, email and any data you are legally required to keep.
☐	Systems requiring backups are identified Computers, servers, Microsoft 365 or Google Workspace, accounting and line-of-business applications, websites.
☐	Backup frequency matches your RPO Data that changes often is backed up often enough that losing the gap would be acceptable.
☐	Backup destinations are recorded You know exactly where each backup is stored, including at least one copy away from your main systems.

How backups are protected

Done	Item
☐	Backups are protected against ransomware At least one copy is offline, immutable or otherwise cannot be changed or deleted from an infected computer.
☐	Backup credentials are kept separate Backup systems use different accounts and passwords from everyday user and administrator accounts, protected with MFA.
☐	Backups are encrypted Backup data is encrypted in transit and at rest, and the encryption key is stored safely and separately.
☐	Retention periods are set You keep enough historical versions to recover from problems found late, and meet any legal retention requirements.

Monitoring and recovery

Done	Item
☐	Backups are monitored Someone reviews backup reports and investigates failures or warnings promptly.
☐	Restoration is tested on a schedule Files, mailboxes and whole systems are test-restored regularly, for example every quarter.
☐	Recovery time objectives are agreed Each critical system has an agreed RTO, and the restoration test shows it can be met.
☐	Recovery point objectives are agreed Each critical system has an agreed RPO that the backup frequency supports.
☐	Responsibilities are assigned A named person is responsible for backups, monitoring and restoration testing, with a backup person.
☐	Incident escalation contacts are recorded You know who to call if a restore fails or data loss is discovered.

Most recent restoration test

Date of test

Tested by

What was restored (files, mailbox, system)

Backup source and date restored from

Time taken to restore

Outcome: successful, partial or failed

Issues found and actions taken

Recovery objectives by system

System or data	RTO	RPO	Backup frequency	Backup location	Owner

Need a hand?

Omnicon I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.