

Backup and Restore Testing Checklist

Mark a check after reviewing the evidence. Assign open items an owner and date. This is a planning aid, not a certification.

☐ 01 Choose the information in scope

Identify essential files, applications and relevant cloud data. Confirm what your backup arrangement includes and what needs a separate solution.

Evidence: A scope list confirmed by service owners.

Owner

Target date

☐ 02 Agree what the business can tolerate

Record how much recent information could be lost and how long the selected service could be unavailable. Use these decisions to guide the backup plan.

Evidence: Business-approved recovery needs in plain language.

Owner

Target date

☐ 03 Confirm the schedule and retention

Check that backup frequency and retained versions support those needs. Identify who receives failure alerts and follows them up.

Evidence: A backup schedule and alert ownership record.

Owner

Target date

☐ 04 Keep a protected separate copy

Review an offline, offsite or appropriately isolated copy so one failure does not affect every backup. Confirm how that protection works in your chosen service.

Evidence: A documented copy location and separation method.

Owner

Target date

☐ 05 Restrict backup administration

Limit backup access to authorized people. Protect administrator accounts and check whether ordinary production credentials could alter or delete every copy.

Evidence: A backup access review and an owner for gaps.

Owner

Target date

☐ 06 Check encryption and key recovery

Protect sensitive backup information in transit and storage where supported. Confirm that authorized staff can recover the keys or credentials needed to restore it.

Evidence: A reviewed access and key-recovery process, without secret values.

Owner

Target date

Backup and Restore Testing Checklist

Continue the review. Record the result, including gaps and decisions that need follow-up.

☐ 07 Agree a safe test plan

Select a small sample, an approved operator and a separate destination. Confirm that the exercise will not overwrite live information or interrupt normal services.

Evidence: An approved test scope and destination.

Owner

Target date

☐ 08 Recover the sample

Follow the backup provider's supported restore instructions. Record which copy was used, who ran the test and how long the recovery took.

Evidence: A dated test record and actual recovery time.

Owner

Target date

☐ 09 Check that the result is usable

Ask the business owner to open the recovered information and confirm it meets the test's purpose. For applications, include the relevant IT specialist.

Evidence: A usability check and a clear list of missing items.

Owner

Target date

☐ 10 Record what the test proved

Compare the observed result with the agreed recovery needs. State the exercise's limits instead of treating one successful sample as proof of complete recovery.

Evidence: An outcome summary with scope and limitations.

Owner

Target date

☐ 11 Protect information used in the exercise

Handle recovered business information under your normal access and retention rules. Agree how temporary test copies will be secured and removed when appropriate.

Evidence: A documented test-copy handling decision.

Owner

Target date

☐ 12 Resolve gaps and test again

Assign unresolved issues an owner and target date. Repeat the exercise after meaningful changes and at an agreed interval.

Evidence: A follow-up plan and the next test date.

Owner

Target date

Turn checks into next steps.

For planned recovery exercises, not recovery during an active incident. Coordinate with your IT provider and follow an approved incident process if compromise is suspected.

YOUR BUSINESS REVIEW

Review led by Date

Next review

NEXT THREE ACTIONS / OWNER / TARGET DATE

Sources and scope

Cyber Centre: Backing up your information (ITSAP.40.002)

<https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002>

Cyber Centre: Foundational security actions (ITSAP.10.300)

<https://www.cyber.gc.ca/en/guidance/foundational-cyber-security-actions-small-organizations-itsap10300>

Cyber Centre: Baseline controls for small and medium organizations

<https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>

Prepared by Canada NexTech. Source guidance checked October 28, 2026. This independent educational resource is not endorsed by the source organizations. Adapt it with the person responsible for your systems.