Backup and restore verification

Manual | 11 steps | 3 roles | Created Sep 2, 2026 | Updated Sep 2, 2026 | v1

How backups are monitored and, more importantly, restore-tested on a schedule, so recovery is proven rather than assumed.

TRIGGER

Daily for the automated job, and monthly for the restore test.

11 STEPS

1 **IT Administrator confirms the backup job completed and checks the log rather than only the status indicator.**

Daily

A job can report success while silently skipping files it could not read. The log shows what was actually captured.

Completed cleanly: Go to step 2: IT Administrator confirms the backup size is within the expected range for the data set.
Failed or partial: Go to step 8: IT Administrator investigates the failure, reruns the job, and escalates to the IT Lead if it fails again.

2 **IT Administrator confirms the backup size is within the expected range for the data set.**

A backup suddenly much smaller than usual is the classic sign of a source path that moved. The job still says success.

3 **IT Administrator confirms coverage against the list of systems and data that must be backed up.**

Coverage against a written list, reviewed when systems are added. New systems not added to the backup scope are the most common gap, and nobody notices until the restore.

All in scope covered: Go to step 4: IT Administrator confirms at least one copy is held off-site or in a separate account, and is not writable from the primary environment.
Gap found: Go to step 9: IT Administrator adds the missing system to the backup scope and records why it was missing.

4 **IT Administrator confirms at least one copy is held off-site or in a separate account, and is not writable from the primary environment.**

Separation is what makes a backup survive ransomware or a compromised admin account. A backup reachable with the same credentials as production is not a backup.

5 **IT Administrator performs a restore test to an isolated location, restoring real data rather than checking the job would run.**

Monthly

Actually restore, to somewhere isolated. This is the only step that proves anything, and it is the one that gets deferred indefinitely.

Restore succeeded: Go to step 6: System Owner confirms the restored data is complete and usable, opening records and checking the most recent entries.

Restore failed: Go to step 10: IT Lead treats the failed restore as an incident, identifies the cause, and sets a date for a re-test.

6 System Owner confirms the restored data is complete and usable, opening records and checking the most recent entries.

The system owner checks usability, not IT. A technically successful restore of subtly corrupted data still fails the business.

Usable: Go to step 7: IT Administrator records the test: date, what was restored, how long it took, and who verified it.
Incomplete or corrupt: Go to step 10: IT Lead treats the failed restore as an incident, identifies the cause, and sets a date for a re-test.

7 IT Administrator records the test: date, what was restored, how long it took, and who verified it.

Record the elapsed time. That figure is your real recovery time, and it is usually much longer than anyone assumes.

Recorded: Ends the procedure

8 IT Administrator investigates the failure, reruns the job, and escalates to the IT Lead if it fails again.

Two consecutive failures is an incident, not a task. Silent repeated failure is how organisations end up with no usable backup at all.

Rerun succeeded: Go to step 2: IT Administrator confirms the backup size is within the expected range for the data set.
Failed again: Go to step 11: IT Lead escalates repeated backup failure, arranges an interim protection method, and informs whoever owns the risk.

9 IT Administrator adds the missing system to the backup scope and records why it was missing.

Record the cause. It is nearly always a provisioning process that does not include adding new systems to backup, which is the real fix.

Scope corrected: Go to step 4: IT Administrator confirms at least one copy is held off-site or in a separate account, and is not writable from the primary environment.

10 IT Lead treats the failed restore as an incident, identifies the cause, and sets a date for a re-test.

A failed restore is the most serious finding this procedure can produce, because it means the protection you believed in does not exist.

Fixed, re-test scheduled: Go to step 5: IT Administrator performs a restore test to an isolated location, restoring real data rather than checking the job would run.

11 IT Lead escalates repeated backup failure, arranges an interim protection method, and informs whoever owns the risk.

Somebody outside IT needs to know the organisation is currently unprotected. That is a business decision, not a technical one.

Interim protection in place: Go to step 8: IT Administrator investigates the failure, reruns the job, and escalates to the IT Lead if it fails again.

ROLES INVOLVED

IT Administrator | System Owner | IT Lead

REVIEW CADENCE

Quarterly, and immediately after adding any system, changing backup tooling, or any failed restore.

Name the person accountable for this procedure before you put it into use.

CHANGE THESE BEFORE YOU USE IT

- List the systems and data in scope explicitly, and add reviewing that list to your system provisioning procedure.
- Set your recovery point and recovery time objectives, then check whether the elapsed time recorded in step 7 actually meets them.
- Set the restore test frequency by criticality rather than uniformly monthly.
- Confirm where decryption keys and credentials are held and that they are not stored only inside the system being backed up. This is a genuinely common single point of failure.
- Add your retention periods, including any legal minimum, and confirm them with whoever owns your compliance.

This is a free starting point from sendabrief.com, not compliance advice. It is written to be adapted.

Source: https://sendabrief.com/templates/backup-and-restore-verification