

Backup Restore Test Checklist

By Checklister

- ☐ Define the authorized test
 - ☐ Confirm the test authorization and responsible people

Record the approved test scope, system owner, authorized operator, reviewer, test window, and runbook version. Confirm that the existing backup system and proposed test destination are in scope. Resolve missing approvals before any restore activity.
 - ☐ Identify the backup and recovery point to test

Record a safe backup-set reference, source system, backup date or recovery point, and relevant retention or availability information. Have the operator confirm that the selected backup is accessible and appropriate for this test. Preserve the source backup and do not assume the newest job is the required recovery point.
 - ☐ Choose the sample and acceptance checks

Before the test, identify each sample and its expected usable result. Examples to adapt: a document opens with known content; an export has the agreed columns/count; selected application records match approved reference values. State exclusions and dependencies. Rename, remove or duplicate the validation examples below to match this inventory.
 - ☐ Agree the timing record and stop conditions

Define the test start and end points, any target for usable recovery, and the checkpoints to record. Agree who can stop the test and which conditions require it, including an uncertain target, unexpected live-system connection, data exposure, or an action outside the approved scope.
- ☐ Confirm isolation and execute
 - ☐ Verify the isolated restore destination

Have the operator confirm the exact approved target, sufficient capacity, restricted access, and isolation required by the runbook. Verify that the restore cannot overwrite production data and that recovered services cannot contact real users or production systems. Stop if any part of the target or isolation cannot be confirmed. Record the target reference and verification evidence. This answer records the check; the separate final source/target safety action below must remain open if anything is uncertain.
 - ☐ Confirm required restore access and prerequisites

Have authorized staff verify the permitted restore access, compatible tools or versions, and required dependencies. Confirm that needed credentials or recovery keys can be used through the approved secure process without copying them into the checklist. Resolve missing prerequisites before starting.
 - ☐ Perform the final source and target safety check

Immediately before execution, confirm the backup reference, recovery point, sample selection, target, and restore options against the approved plan. Check that the planned action changes only the authorized test destination. Record the operator's go/no-go decision and do not proceed if the scope or impact has changed. Leave this action unchecked and do not execute the restore unless the source, exact target, isolation, authorization and prerequisites are confirmed.
 - ☐ Restore the agreed sample through the approved runbook

Have the authorized operator perform the restore into the verified isolated target using the existing system-specific procedure. Record the start time, job reference, completion time, and status. Follow the stop conditions for unexpected behavior; do not improvise production changes or repeat an uncertain job without checking its state.
 - ☐ Record the restore start time

Enter the actual timestamp using the same stated timezone for all checkpoints.
 - ☐ Record the restore completion time

Record completion only after checking the job state; if it failed or stopped, record that actual endpoint and explain it in the job notes.
- ☐ Validate the recovered samples
 - ☐ Check recovered items against the sample inventory

Compare the recovered files or records with the agreed inventory and recovery-point expectations. Check the expected locations, counts, and relevant metadata, and identify missing or unexpected items. Where the runbook provides a checksum or other integrity method, record its result and evidence rather than assuming matching names prove integrity.
 - ☐ Open and validate the recovered sample

Editable validation examples: rename for the real samples, remove irrelevant types and duplicate for independently checked samples. Use only the approved isolated environment. On each result record the safe sample reference, expected/actual detail and evidence in task notes; do not paste recovered private content.
 - ☐ Starter sample: open a recovered document

Replace with an approved representative file. Confirm it opens and the expected known content is readable; a matching filename alone is insufficient.

- ☐ **Optional sample: validate a recovered export or folder**
Replace or remove. Compare agreed paths, columns/counts or reference values and use the runbook's integrity check where provided.
- ☐ **Optional sample: validate isolated application records**
Replace or remove. Have the authorized operator run the approved read-only application check with live integrations unavailable. Verify the chosen reference records and dependencies.
- ☐ **Record the validation completion time**
Enter only when the agreed validation pass has finished. An unfinished validation remains blank and is reported as incomplete.
- ☐ **Record restore time and validation results**
Using the recorded timestamps, calculate restore duration and time to validated usability with their defined start/end points. State waiting or prerequisite delays, compare only with a target for the same scope, and link restricted logs. Do not report a completed job as usable recovery without validation.
- ☐ **Resolve, clean up and report**
 - ☐ **Resolve failed checks and verify required retests**
For each failure or untested acceptance check, add a separate named follow-up action with the safe sample reference, impact, evidence, investigation owner and next date. Record remediation approval through normal change control. Keep this action open until required retests are verified, or link the formally accepted remaining limitation and its owned follow-up.
 - ☐ **Complete the approved handling of test copies**
Have the authorized operator carry out the agreed retention or cleanup procedure for recovered test data and temporary resources. Verify the exact test targets before any removal and preserve source backups and required evidence. Record what was retained or removed and confirm no unintended test access or running integration remains.
 - ☐ **Review the scoped outcome and next test**
Have the reviewer record whether this sample test passed, failed, or remains incomplete, with the backup reference, recovery point, limitations, and evidence. Confirm that cleanup is accounted for and every open issue has an owner and next date. Agree the next test or retest through the organization's existing process without treating this result as a recovery guarantee.