

How to document a backup recovery test

[Czytaj po polsku](#)

A readable backup file is only the start: verify restoration of a usable service.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Define the scenario and acceptance criteria

Choose a specific service and recovery point. Agree tolerable data loss and restoration time: RPO and RTO. Test in an isolated environment or approved work window without risking production data.

Restore dependencies

Recovery may require configurations, keys, accounts, DNS and dependent applications as well as data. Keep secrets out of public test records. Check service startup and an agreed business operation; a matching archive checksum does not prove the application works.

Record results and corrective action

Record the backup, dates, timings, scope, operator, test outcomes and limitations. Do not describe a partial exercise as a test of every system. Assign fixes and retests for failures. Protect backups from incidents affecting the production environment.

Practical checklist

- Scenario, RPO and RTO.
- Safe test environment.
- Functional check by the service owner.
- Record, limitations and corrective actions.

Next steps and references

[DATPOL service scope and supporting material](#)

[CISA — StopRansomware Guide](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to prepare a business for an audit without disrupting operations](#)
- [How to compare an indoor server room with a container solution](#)
- [What to prepare before connecting a public authority to a SOC](#)

Revision #2

Created 2026-10-04 14:56:34 UTC by Administrator DATPOL

Updated 2026-10-04 14:56:35 UTC by Administrator DATPOL