Sample audit programme

BSI baseline protection

Backup and recovery

13 audit steps · BSI baseline protection

13 audit steps with criterion, reference, procedure and expected evidence. 8 documents to request and the typical findings.

BSI CON.3 · BSI DER.4 · NIS2 Directive Art. 21(2)(c) · ISO/IEC 27001:2022 Annex A 8.13 · ISO/IEC 27001:2022 Annex A 5.23 · NIS2 Directive Art. 21(2)(f)

Audit objective and scope

The audit assesses whether the organisation backs up data and systems so that they can be restored after an outage, an error or an attack within the required time and to the required data state. What matters is evidence that recovery works, not only that backups run.

SCOPE

- Servers, virtual machines, databases, business applications and file storage in the data centre and, where relevant, at sites
- Data in cloud and SaaS services, where the organisation is responsible for backing it up
- Backup software, storage systems, media and storage locations
- Out of scope: archiving to meet retention obligations, unless agreed separately

Audit steps 1 to 3

Step 01 — BSI CON.3

A data backup concept exists, is approved and is current.

Procedure Read the concept, establish approval and date of the last review, and ask who is responsible.

Evidence Data backup concept with approval record and version

Step 02 — BSI CON.3; BSI DER.4

Tolerable data loss and recovery time per system are derived from the requirements of the business processes.

Procedure Compare the targets per system with the results of the impact analysis and ask about deviations.

Evidence Overview of targets per system, impact analysis

Step 03 — BSI CON.3

All relevant systems and data are included in the backup.

Procedure Compare the system overview and the configuration management with the backup jobs and identify systems that are not backed up.

Evidence System overview, list of backup jobs

Audit steps 4 to 6

Step 04

BSI CON.3

Methods, schedules and retention of backups correspond to the requirements of the concept.

Procedure For a sample of systems, compare the configuration of the backup jobs with the concept.

Evidence Extract of job configuration, concept

Step 05

BSI CON.3

Backup runs are monitored, errors are handled and closed in a traceable way.

Procedure Review the logs of one month, select failed runs and follow their handling through to closure.

Evidence Backup logs, notifications and tickets for failed runs

Step 06

BSI CON.3; NIS2 Directive Art. 21(2)(c); ISO/IEC 27001:2022 Annex A 8.13

Backups are protected against manipulation and encryption by malware, for example through separate credentials and immutable or separately stored copies.

Procedure Check access rights to the backup system and media and establish whether at least one copy cannot be changed from the production environment.

Evidence Authorisation extract, architecture overview, configuration of immutable storage

Audit steps 7 to 9

Step 07 — BSI CON.3

Backup media and stored backups are protected against unauthorised access and encrypted where needed.

Procedure Check encryption settings and access rights and review key management.

Evidence Configuration extract, key management concept

Step 08 — BSI CON.3

At least one copy is stored at a location physically separate from the production system.

Procedure Review the storage locations and assess the physical and organisational separation.

Evidence List of copy locations, site visit note or provider evidence

Step 09 — BSI CON.3; ISO/IEC 27001:2022 Annex A 8.13

Restores are tested regularly; the result and the time required are compared with the targets.

Procedure Check the test plan and test records of the last twelve months and, where possible, observe a restore.

Evidence Test plan, test records with time measurement, deviation reports

Audit steps 10 to 13

Step 10 — BSI CON.3; BSI DER.4

The recovery procedure is documented, owners are named and the documentation is available even if the main environment fails.

Procedure Read the manual, check where it is stored and establish whether the documents are accessible offline.

Evidence Recovery manual, list of owners, storage concept

Step 11 — BSI CON.3

Retention and deletion periods for backups are defined and observed.

Procedure Compare the periods with the settings of the backup software and the existing stock.

Evidence Retention rules, extract of backup inventory

Step 12 — ISO/IEC 27001:2022 Annex A 5.23

For cloud and SaaS services it is clear who backs up which data, and the provider commitment can be evidenced.

Procedure Read contracts and service descriptions on data backup and request evidence of backup and recovery.

Evidence Contract extracts, service description, provider confirmations

Step 13 — NIS2 Directive Art. 21(2)(f)

Those responsible regularly receive metrics on success rate, test results and open deficiencies.

Procedure Review the reports of the last twelve months and follow up actions on deficiencies found.

Evidence Reports, action list

Document request list

Request these 8 documents before you start

1. Data backup concept and recovery manual
2. Targets for tolerable data loss and recovery time per system
3. System overview and list of backup jobs
4. Backup logs of one continuous month
5. Test plan and test records of restores
6. Authorisation extract for the backup system and media
7. Contracts and service descriptions of cloud and backup providers
8. Reports on backup metrics

TYPICAL FINDINGS

- Restore tests never took place or covered only single files, not complete systems.
- New systems have not been added to the backup.
- The backup system can be reached with the same administrator accounts as production.
- There is no copy that is protected against encryption by malware.
- Failed runs are not followed up; some systems have been without a valid backup for weeks.
- The measured recovery time is clearly above the target of the business unit.

Sample audit programme library

29 sample audit programmes online

proauditmap.com/en/audit-programs/

Full audit package in ProAuditMap

proauditmap.com

ProAuditMap

Sample provided without warranty and not legal advice. Laws, regulations and standards appear only as references, no normative text is reproduced. Adapt scope and depth to your organisation, your risks and the current version of the provisions that apply to you before use.
Last updated: 13 October 2026