Sample audit programme

Critical infrastructure

Evidence audit

11 audit steps · BSIG

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

§ 31(1) and (2) BSIG · § 30(2) no. 1 BSIG · NIS2 Directive Art. 20 · § 31(1) BSIG · § 31(2) BSIG · § 30(2) no. 2 and 3 BSIG · § 30(2) no. 4 BSIG · § 30(2) no. 9 and 10 BSIG · § 30(2) no. 6 BSIG · § 32(1) BSIG · § 39(1) BSIG

Audit objective and scope

The audit assesses whether an operator of critical facilities has implemented the risk management measures for its critical facilities that go beyond the general level, whether attack detection systems are operated and whether reporting duties can be met. It also assesses whether the proof for the Federal Office through audits, inspections or certifications is prepared: scope, auditors, documentation and handling of deficiencies.

SCOPE

- Critical facilities of the operator and the IT systems, components and processes needed to run them
- Risk management measures under the general and the special requirements for operators of critical facilities
- Preparation and performance of the proof to the Federal Office
- Out of scope: physical resilience measures under the KRITIS umbrella act and sector-specific requirements, unless agreed separately

Audit steps 1 to 3

Step 01 § 31(1) and (2) BSIG

The operator's critical facilities are determined and delimited; the IT systems, components and processes needed to run them are known and documented.

Procedure Compare the delimitation of critical facilities and the list of associated systems with the system overview.

Evidence Documentation of critical facilities, system overview, dependency overview

Step 02 § 30(2) no. 1 BSIG; NIS2 Directive Art. 20

A risk analysis with security concepts exists for the critical facilities; it is current and owned by management.

Procedure Read the risk analysis and security concepts and check currency and approval by management.

Evidence Risk analysis, security concepts, management approval records

Step 03 § 31(1) BSIG

For the critical facilities the measures go beyond the general level and the effort is not disproportionate to the consequences of a failure.

Procedure Check how the proportionality of measures for the critical facilities is justified and documented.

Evidence Justification of proportionality, catalogue of measures for the critical facilities

Audit steps 4 to 6

Step 04 § 31(2) BSIG

Attack detection systems are used that continuously and automatically collect and evaluate suitable parameters and identify ongoing threats.

Procedure Review the systems, components covered and evaluation, and check coverage of the systems of the critical facilities.

Evidence Architecture of attack detection, coverage overview, evaluations

Step 05 § 30(2) no. 2 and 3 BSIG

Measures for handling security incidents and for maintaining operations are implemented and exercised.

Procedure Read incident and continuity plans for the critical facilities and review the results of the last exercise.

Evidence Incident and continuity plans, exercise records

Step 06 § 30(2) no. 4 BSIG

The supply chain of the critical facilities is considered; providers with access are bound by contract to security requirements.

Procedure Check contracts and assessments of three providers of the critical facilities.

Evidence Provider inventory, contracts, assessments

Audit steps 7 to 9

Step 07 § 30(2) no. 9 and 10 BSIG

Access control and multi-factor authentication are implemented for the systems of the critical facilities.

Procedure Check authorisations and authentication for the systems of the critical facilities in a sample.

Evidence Authorisation extracts, configuration of multi-factor authentication

Step 08 § 30(2) no. 6 BSIG

Concepts and procedures for assessing the effectiveness of the measures exist and are applied.

Procedure Review the effectiveness assessment procedure and the results of the last twelve months.

Evidence Audit plan, effectiveness assessment reports, action list

Step 09 § 32(1) BSIG

Significant security incidents can be reported to the joint reporting office: early warning within 24 hours, notification within 72 hours, final report after one month.

Procedure Check the reporting process, responsibilities and templates, and examine a report or exercise for compliance with the deadlines.

Evidence Reporting process, templates, evidence of exercise or report

Audit steps 10 to 11

Step 10 § 39(1) BSIG

The proof to the Federal Office is planned: scope, type of proof (audit, inspection or certification), date within the three-year cycle and auditors are defined.

Procedure Compare the proof planning with the date set by the Federal Office and check the suitability and independence of the audit body.

Evidence Proof planning, engagement of the audit body, notice of date from the Federal Office

Step 11 § 39(1) BSIG

Security deficiencies found are recorded with deadline and owner, tracked and demonstrably remedied towards the Federal Office.

Procedure Review deficiency lists from earlier proofs and check the state of remediation.

Evidence Deficiency list, action plan, evidence of remediation

Document request list

Request these 8 documents before you start

1. Documentation of the critical facilities and associated systems
2. Risk analysis and security concepts
3. Justification of the proportionality of measures
4. Description of attack detection with coverage overview
5. Incident and continuity plans with exercise records
6. Reporting process with templates and responsibilities
7. Proof planning and reports of earlier audits, inspections or certifications
8. Deficiency list with action plan

TYPICAL FINDINGS

The delimitation of the critical facilities and the necessary IT systems is not current, and dependencies are not recorded.

Attack detection does not cover part of the systems of the critical facilities.

The proportionality of measures is not justified, and special measures for the critical facilities are not apparent.

The ability to report has never been exercised, and deputies for the responsible people are not clarified.

The proof is prepared too late, and the scope of the audit does not fully cover the critical facilities.

Deficiencies from earlier audits have no deadline or owner and are not tracked.

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