Sample audit programme

Patch and vulnerability management

13 audit steps · NIS2, ISO 27001

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

BSI OPS.1.1.3 · ISO/IEC 27001:2022 Annex A 8.8 · ISO/IEC 27001:2022 Annex A 5.9 · NIS2 Directive Art. 21(2)(f) · NIS2 Directive Art. 21(2)(e)

Audit objective and scope

The audit assesses whether the organisation systematically detects known vulnerabilities in systems and software, assesses them by risk and fixes them in time, and whether exceptions are handled in a controlled and traceable way. It also assesses whether the patch level is evidenced by reports.

SCOPE

- Servers, workstations, network and security components, databases and applications under the organisation's responsibility
- Firmware, third-party software and libraries, where used in in-house development
- Vulnerability scans and the procedures for assessment, testing, deployment and exceptions
- Out of scope: penetration tests, unless agreed separately; systems fully operated by a provider, other than through the steering of that provider

Audit steps 1 to 3

Step 01

BSI OPS.1.1.3; ISO/IEC 27001:2022 Annex A 8.8

A patch and vulnerability management process exists, is approved and sets deadlines by criticality.

Procedure Read the process description and check whether deadlines, roles, exceptions and escalation are defined.

Evidence Process description with approval, deadline matrix

Step 02

ISO/IEC 27001:2022 Annex A 5.9

A current inventory of systems and installed software serves as the basis.

Procedure Compare the inventory with a network scan or directory data and identify systems not recorded.

Evidence Inventory, comparison list

Step 03

BSI OPS.1.1.3

Sources of vulnerability information are defined and evaluated by named people.

Procedure Ask for the sources and owners and, for a recent vulnerability, trace the path from notification to assessment.

Evidence List of sources, responsibilities, assessment note for an example

Audit steps 4 to 6

Step 04

BSI OPS.1.1.3; ISO/IEC 27001:2022 Annex A 8.8

New vulnerabilities are assessed for relevance and risk and the assessment is documented.

Procedure Select five highly critical vulnerabilities from one quarter and trace the assessment.

Evidence Assessment records, tickets

Step 05

ISO/IEC 27001:2022 Annex A 8.8

Vulnerability scans run regularly and cover the systems in scope.

Procedure Compare the scan plan and scan ranges with the inventory and review the latest reports.

Evidence Scan plan, scan reports, coverage overview

Step 06

BSI OPS.1.1.3

Critical vulnerabilities are fixed within the defined deadline and overruns are followed up.

Procedure For a sample of critical vulnerabilities, determine the time from awareness to remediation and compare it with the deadline.

Evidence Evaluation of open and closed vulnerabilities, tickets, escalations

Audit steps 7 to 9

Step 07 BSI OPS.1.1.3

Patches are tested before deployment in production and fallback options exist.

Procedure Trace the testing and approval flow for two recent patches.

Evidence Test records, approvals, fallback plan

Step 08 BSI OPS.1.1.3; ISO/IEC 27001:2022 Annex A 8.8

Exceptions are justified, approved by a competent body, time-limited and backed by compensating measures.

Procedure Review the list of exceptions and, for a sample, check justification, approval, time limit and compensating measures.

Evidence Exception list with approvals and compensating measures

Step 09 BSI OPS.1.1.3

Systems and software without vendor support are identified and handled under a plan.

Procedure Filter the inventory for unsupported systems and review the plans for replacement or protection.

Evidence List of unsupported systems, replacement plans, risk acceptance

Audit steps 10 to 13

Step 10 — ISO/IEC 27001:2022 Annex A 8.8

The patch level covers all kinds of components: operating systems, applications, network devices, firmware and third-party software.

Procedure Review patch level reports per component type and identify gaps in coverage.

Evidence Patch level reports, coverage overview

Step 11 — NIS2 Directive Art. 21(2)(f)

Effectiveness is evidenced by repeated scans or patch level reports.

Procedure For remediated vulnerabilities, check whether a repeated scan confirms success.

Evidence Follow-up scans, closure notes

Step 12 — NIS2 Directive Art. 21(2)(f)

Metrics on patch level and compliance with deadlines are reported to those responsible and lead to action.

Procedure Read the reports of the last twelve months and trace the decisions on deviations.

Evidence Metric reports, minutes, action lists

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

For vulnerabilities in the entity's own products and services there is, where applicable, a procedure to receive and handle reports.

Procedure Check the reporting channel, responsibilities and the handling of an example.

Evidence Procedure description, contact address, handling record

Document request list

Request these 8 documents before you start

1. Process description for patch and vulnerability management with deadline matrix
2. Inventory of systems and software
3. Scan plan and vulnerability reports of recent quarters
4. Evaluation of open and closed vulnerabilities with time to remediation
5. Patch level reports per component type
6. List of exceptions with approvals and compensating measures
7. List of systems without vendor support and replacement plans
8. Metric reports to those responsible

TYPICAL FINDINGS

- The inventory is incomplete, so systems are missing from the scan and the patch process.
- Deadlines are defined but regularly exceeded for critical vulnerabilities, without escalation.
- Network devices and firmware are not part of the patch process.
- Exceptions run without end date and without compensating measures.
- Systems without vendor support are in operation and no replacement plan exists.
- Remediation is not confirmed by a repeated scan.

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