Sample audit programme

Secure software development

12 audit steps · ISO 27001, BSI, NIS2

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

ISO/IEC 27001:2022 Annex A 8.25 · BSI CON.8 · ISO/IEC 27001:2022 Annex A 8.26 · BSI APP.3.1 · ISO/IEC 27001:2022 Annex A 8.27 · ISO/IEC 27001:2022 Annex A 8.28 · ISO/IEC 27001:2022 Annex A 8.28 and 8.29 · ISO/IEC 27001:2022 Annex A 8.29 · NIS2 Directive Art. 21(2)(e) · § 30(2) no. 5 BSIG · ISO/IEC 27001:2022 Annex A 8.31 · ISO/IEC 27001:2022 Annex A 8.4 · ISO/IEC 27001:2022 Annex A 8.32 · ISO/IEC 27001:2022 Annex A 8.30

Audit objective and scope

The audit assesses whether the organisation runs a development process that takes security into account from the start: requirements, architecture principles, secure coding, review and testing before release, protection of source code and development environments, and governance of outsourced development. It also assesses whether vulnerabilities in own software are handled.

SCOPE

- In-house developments and customised software, including web applications, interfaces and operational scripts
- Development, test and deployment processes, tools and environments
- Outsourced development by service providers
- Out of scope: standard software without customisation and change control in operations, which is covered in a separate sample

Audit steps 1 to 3

Step 01 ISO/IEC 27001:2022 Annex A 8.25; BSI CON.8

A framework for the development process with security requirements for each phase is defined, approved and applied.

Procedure Read the process description and check on two projects whether the security requirements per phase were implemented.

Evidence Development policy, project documents of the sample

Step 02 ISO/IEC 27001:2022 Annex A 8.26; BSI APP.3.1

Security requirements are gathered at the start for each application, agreed and tracked, including for interfaces and data.

Procedure Review the requirements documents of three applications for security requirements and their implementation.

Evidence Requirements documents, traceability to testing

Step 03 ISO/IEC 27001:2022 Annex A 8.27

Architecture and engineering principles for secure systems are defined and are applied and reviewed for new systems.

Procedure Read the architecture guidelines and trace their application for two new systems.

Evidence Architecture guidelines, design documents, decision notes

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 8.28

Binding rules exist for secure coding, which developers know and apply; training is evidenced.

Procedure Review the coding guideline, training records and examples from code review.

Evidence Coding guideline, training records, code review records

Step 05 — ISO/IEC 27001:2022 Annex A 8.28 and 8.29

Changes to source code are reviewed by a second person before they reach the main branch; static analysis tools are in use.

Procedure Select ten changes and check that review by a second person and a run of the analysis tools are evidenced.

Evidence Extract of change requests, results of analysis tools

Step 06 — ISO/IEC 27001:2022 Annex A 8.29; NIS2 Directive Art. 21(2)(e)

Security testing is part of development and acceptance: testing for vulnerabilities, dependencies and configuration before release.

Procedure Check test plans, results and handling of findings for two releases.

Evidence Test plans, test reports, release records

Audit steps 7 to 9

Step 07

NIS2 Directive Art. 21(2)(e); § 30(2) no. 5 BSIG

Known vulnerabilities in libraries and components are detected, assessed and fixed; the components in use are recorded.

Procedure Review the procedure for recording and checking dependencies and trace the handling of findings of the last six months.

Evidence Component list, dependency check reports, action list

Step 08

ISO/IEC 27001:2022 Annex A 8.31

Development, test and production are separated, and production data is not used in tests or only in protected form.

Procedure Check environments and access rights and establish whether test environments contain production data.

Evidence Environment overview, authorisation extract, procedure on test data

Step 09

ISO/IEC 27001:2022 Annex A 8.4

Access to source code and development tools is limited to authorised people and logged; credentials and keys are not stored in source code.

Procedure Read permissions on repositories and build systems and search source code for stored credentials.

Evidence Authorisation extract, result of secret search, logs

Audit steps 10 to 12

Step 10 ISO/IEC 27001:2022 Annex A 8.32; BSI CON.8

Deployment to production follows a controlled flow with approval, not direct intervention by individuals.

Procedure Compare deployment logs of the last three months with approvals.

Evidence Deployment logs, approvals, rights on production systems

Step 11 ISO/IEC 27001:2022 Annex A 8.30

For outsourced development, security requirements are fixed by contract, compliance is monitored and the result is checked.

Procedure Check contracts and acceptances of two outsourced developments, in particular audit rights and rights to source code.

Evidence Contracts, acceptance records, audit reports

Step 12 NIS2 Directive Art. 21(2)(e)

Vulnerabilities in own software are reported, assessed and fixed; there is a way to receive reports from outside.

Procedure Check the procedure for handling reported vulnerabilities and how the latest reports were processed.

Evidence Procedure, reporting channel, vulnerability register

Document request list

Request these 8 documents before you start

1. Policy on secure development and the development process
2. Coding guideline and training records
3. Requirements documents of the sample with security requirements
4. Architecture guidelines and design documents
5. Extract of change requests with review notes
6. Test plans, test reports and release records
7. Authorisation extract for repositories and build systems
8. Contracts and acceptances of outsourced development

TYPICAL FINDINGS

- Security requirements are considered only shortly before release, not at the start.
- Changes reach the main branch without review by a second person.
- Credentials and keys are stored in source code.
- Known vulnerabilities in libraries are not detected systematically, and the components in use are not recorded.
- Test environments contain unchanged production data.
- Contracts with development providers regulate neither audit rights nor rights to source code.

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