Sample audit programme

Security awareness and training

13 audit steps · NIS2, ISO 27001, BSI

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

BSI ORP.3 · ISO/IEC 27001:2022 Annex A 6.3 · DORA Art. 13(6) · ISO/IEC 27001:2022 clause 7.3 · NIS2 Directive Art. 20(2) · § 38(3) BSIG · NIS2 Directive Art. 21(2)(g) · § 30(2) no. 7 BSIG · ISO/IEC 27001:2022 clause 7.2 · ISO/IEC 27001:2022 clause 9.1 · ISO/IEC 27001:2022 Annex A 6.8 · Art. 39(1)(b) GDPR · DORA Art. 5(2)(g)

Audit objective and scope

The audit assesses whether the organisation has a concept for information security awareness and training that reaches all target groups, including management, IT staff and service providers. It also assesses whether participation is tracked, effectiveness is measured and reporting of anomalies is encouraged.

SCOPE

- Information security awareness and training offerings for all staff
- Management training and specialist training for IT staff and administrators
- Phishing simulations, learning platform and participation tracking
- Out of scope: general professional training without a security focus

Audit steps 1 to 3

Step 01 — BSI ORP.3; ISO/IEC 27001:2022 Annex A 6.3

A concept governs objectives, target groups, content, formats and frequency of awareness and training.

Procedure Read the concept, check approval and currency and compare it with the training plan for the current year.

Evidence Awareness and training concept, annual plan

Step 02 — DORA Art. 13(6); BSI ORP.3

Content is tailored to the roles and risks of the target groups.

Procedure For three target groups, compare content with the typical risks of their work.

Evidence Training material per target group

Step 03 — ISO/IEC 27001:2022 Annex A 6.3; ISO/IEC 27001:2022 clause 7.3

New staff are briefed before or as soon as they gain access to information; everyone takes part regularly.

Procedure For ten joiners, compare the briefing date with the account creation date.

Evidence Joiner list, attendance records, account creation dates

Audit steps 4 to 6

Step 04 — NIS2 Directive Art. 20(2); § 38(3) BSIG

Members of management attend training on cyber risks regularly.

Procedure Check management attendance records for the last two years and the training content.

Evidence Attendance records, management training material

Step 05 — NIS2 Directive Art. 21(2)(g); § 30(2) no. 7 BSIG

Basic cyber hygiene rules are taught and easy to find.

Procedure Have the rules located on the intranet and ask five employees about key rules.

Evidence Rules of conduct, interview notes

Step 06 — ISO/IEC 27001:2022 clause 7.2

IT staff and administrators receive specialist training that ensures their competence for security tasks.

Procedure Compare competence requirements for two IT roles with training records.

Evidence Competence profiles, training records, certificates

Audit steps 7 to 9

Step 07 — ISO/IEC 27001:2022 Annex A 6.3; BSI ORP.3

Phishing simulations are run regularly, evaluated and linked to learning offers.

Procedure Review results of the latest simulations: click rate, report rate and follow-up actions.

Evidence Simulation analyses, follow-up training

Step 08 — ISO/IEC 27001:2022 Annex A 6.3

Participation is tracked; outstanding mandatory training is reminded and escalated.

Procedure Retrieve participation rates per department and trace the handling of those who are overdue.

Evidence Participation report, reminders, escalations

Step 09 — ISO/IEC 27001:2022 clause 9.1

The effectiveness of the measures is measured and fed back into planning.

Procedure Review effectiveness metrics and check whether results led to changes in the programme.

Evidence Metrics report, changes to the training plan

Audit steps 10 to 13

Step 10 — ISO/IEC 27001:2022 Annex A 6.8

Staff know the reporting path for security events and use it.

Procedure Analyse the number of reports over time and ask five employees about the reporting path.

Evidence Reporting statistics, interview notes

Step 11 — DORA Art. 13(6)

Service providers with access to systems or information are included in awareness activities.

Procedure Check contracts and attendance records for two providers with access.

Evidence Contract clauses, provider attendance records

Step 12 — Art. 39(1)(b) GDPR

Data protection training is coordinated with the data protection officer.

Procedure Ask about coordination of content and responsibilities between information security and data protection.

Evidence Data protection training plan, coordination record

Step 13 — DORA Art. 5(2)(g)

Budget and owners are defined for awareness and training.

Procedure Review the programme budget and resources and compare them with the scope of the annual plan.

Evidence Budget plan, role description

Document request list

Request these 8 documents before you start

1. Awareness and training concept
2. Annual training plan
3. Training material per target group
4. Participation reports per department
5. Management attendance records
6. Phishing simulation analyses
7. Effectiveness metrics
8. Reporting statistics for security events

TYPICAL FINDINGS

- Training is the same for everyone and ignores roles.
- New staff gain access weeks before their first training.
- Management is exempt from mandatory training.
- Participation rates are low, overdue staff are not followed up.
- Phishing simulations are run but not evaluated.
- Service providers with administrator access are not included.

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