Sample audit programme

ISMS under ISO/IEC 27001

13 audit steps · ISO 27001, BSI

13 audit steps with criterion, reference, procedure and expected evidence. 9 documents to request and the typical findings.

ISO/IEC 27001:2022 clauses 4.1 and 4.2 · ISO/IEC 27001:2022 clause 4.3 · ISO/IEC 27001:2022 clauses 5.1 and 5.2 · BSI standard 200-1 · ISO/IEC 27001:2022 clause 5.3 · ISO/IEC 27001:2022 clauses 6.1 and 8.2 · BSI standard 200-3 · ISO/IEC 27001:2022 clauses 6.1.3 and 8.3 · ISO/IEC 27001:2022 clause 6.2 · ISO/IEC 27001:2022 clauses 7.1, 7.2 and 7.3 · ISO/IEC 27001:2022 clause 7.5 · ISO/IEC 27001:2022 clause 9.1 · ISO/IEC 27001:2022 clause 9.2 · ISO/IEC 27001:2022 clause 9.3 · ISO/IEC 27001:2022 clauses 10.1 and 10.2

Audit objective and scope

The audit assesses whether the organisation has established an information security management system that links context, scope, leadership, risk assessment and treatment, support, operation, evaluation and improvement coherently. It also assesses whether internal audit and management review lead to decisions and corrective actions.

SCOPE

- Information security management system within the defined scope
- Processes of clauses 4 to 10 of ISO/IEC 27001:2022, including the statement of applicability
- Roles of top management, the information security officer and process owners
- Out of scope: in-depth testing of individual Annex A controls, which have their own audit programmes

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 clauses 4.1 and 4.2

Internal and external issues and the requirements of interested parties are determined and kept current.

Procedure Read the context analysis and list of interested parties and check that legal and contractual requirements are included.

Evidence Context analysis, list of interested parties and their requirements

Step 02 — ISO/IEC 27001:2022 clause 4.3

The scope is documented, justified and takes interfaces and dependencies into account.

Procedure Reconcile the scope with the organisation chart, sites and outsourced services.

Evidence Scope document, site list, interface description

Step 03 — ISO/IEC 27001:2022 clauses 5.1 and 5.2; BSI standard 200-1

Top management demonstrates leadership, has approved an information security policy and ensures it is communicated.

Procedure Read the policy, check approval and ask management in interview about its involvement in the management system.

Evidence Information security policy, communication record, interview notes

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 clause 5.3

Roles, responsibilities and authorities in the management system are assigned and communicated.

Procedure Review the appointment of the information security officer and role descriptions and trace the reporting line to management.

Evidence Letter of appointment, role descriptions, reporting line

Step 05 — ISO/IEC 27001:2022 clauses 6.1 and 8.2; BSI standard 200-3

A defined risk assessment process produces repeatable results and is applied at planned intervals and after changes.

Procedure Read the method description and check the last risk assessment for rating and justification of three risks.

Evidence Risk assessment method, risk register, date of last assessment

Step 06 — ISO/IEC 27001:2022 clauses 6.1.3 and 8.3

A risk treatment plan and a statement of applicability exist; residual risks are accepted by the risk owners.

Procedure Check the statement of applicability for justified exclusions and trace risk acceptance for three residual risks.

Evidence Statement of applicability, risk treatment plan, acceptance records

Audit steps 7 to 9

Step 07

ISO/IEC 27001:2022 clause 6.2

Measurable security objectives are set and planned with owners, resources and deadlines.

Procedure Review the objectives overview and check measurement, owners and achievement for three objectives.

Evidence Objectives overview, status reports on objectives

Step 08

ISO/IEC 27001:2022 clauses 7.1, 7.2 and 7.3

Resources are provided; people with security tasks are competent, and staff know their contribution.

Procedure Review competence evidence for two key roles and ask five employees about their knowledge of the policy.

Evidence Qualification records, training plan, interview notes

Step 09

ISO/IEC 27001:2022 clause 7.5

Documented information is controlled: approval, versioning, distribution and retention are governed.

Procedure Check version, approval and storage location for five documents of the management system.

Evidence Document control rule, document register

Audit steps 10 to 13

Step 10 — ISO/IEC 27001:2022 clause 9.1

Performance and effectiveness of the management system are monitored, measured and evaluated.

Procedure Review definitions of measures, methods and timing and check the latest evaluations.

Evidence Measurement concept, evaluations, metrics reports

Step 11 — ISO/IEC 27001:2022 clause 9.2

Internal audits are carried out under a programme by objective auditors, and results are reported to management.

Procedure Check the audit programme of the last three years for coverage of the scope and review two audit reports.

Evidence Audit programme, audit reports, evidence of auditor independence

Step 12 — ISO/IEC 27001:2022 clause 9.3

Top management reviews the management system at planned intervals with the required inputs and takes documented decisions.

Procedure Check the minutes of the last management review for inputs, outputs and decisions.

Evidence Management review minutes, list of decisions

Step 13 — ISO/IEC 27001:2022 clauses 10.1 and 10.2

Nonconformities are addressed at the root cause, corrective actions are checked for effectiveness and the management system is improved continually.

Procedure Follow five nonconformities from audits or incidents from root cause analysis to effectiveness check.

Evidence Nonconformity register, root cause analyses, effectiveness evidence

Document request list

Request these 9 documents before you start

1. Context analysis and list of interested parties
2. Scope document
3. Information security policy and role descriptions
4. Risk assessment method, risk register and risk treatment plan
5. Statement of applicability
6. Security objectives with status reports
7. Audit programme and internal audit reports
8. Minutes of the last management review
9. Register of nonconformities and corrective actions

TYPICAL FINDINGS

- The statement of applicability excludes controls without justification.
- The risk assessment has not been repeated for years, not even after major changes.
- Security objectives are not measurable.
- The audit programme does not cover the scope, auditors audit their own work.
- The management review is a short note without inputs and without decisions.
- Corrective actions are closed without checking their effectiveness.

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