Sample audit programme

IT governance and IT strategy

12 audit steps · NIS2, DORA, BSIG

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

DORA Art. 6(8) · NIS2 Directive Art. 20(1) · § 38(1) BSIG · ISO/IEC 27001:2022 Annex A 5.2 · DORA Art. 5(2)(c) · DORA Art. 6(8)(b) · DORA Art. 6(8)(c) · DORA Art. 5(2)(g) · ISO/IEC 27001:2022 Annex A 5.1 · NIS2 Directive Art. 20(2) · § 38(3) BSIG · DORA Art. 5(2)(i) · DORA Art. 6(8)(d) · ISO/IEC 27001:2022 Annex A 5.35 · DORA Art. 6(6) · ISO/IEC 27001:2022 Annex A 5.3

Audit objective and scope

The audit assesses whether an approved IT strategy is derived from business objectives and whether roles, committees, policies, metrics and reporting lines enable effective direction of IT by management. It also assesses whether management approves and oversees the cybersecurity risk management measures and receives training on them.

SCOPE

- IT strategy, IT committees and decision processes of the organisation
- Roles of management, IT leadership, information security and control functions
- Budget and resource planning, metrics and reporting to management
- Out of scope: the technical audit of individual projects or systems

Audit steps 1 to 3

Step 01

DORA Art. 6(8)

An IT strategy exists, is derived from the business strategy, approved by management and reviewed regularly.

Procedure Read the strategy, check approval and date, and trace its derivation from business objectives for three objectives.

Evidence IT strategy with approval, business objectives, record of the last review

Step 02

NIS2 Directive Art. 20(1); § 38(1) BSIG

Management approves the cybersecurity risk management measures and oversees their implementation.

Procedure Review minutes of management meetings for the last twelve months for approvals, reports and decisions on security.

Evidence Meeting minutes, decision papers, status reports

Step 03

ISO/IEC 27001:2022 Annex A 5.2; DORA Art. 5(2)(c)

Roles, responsibilities and authorities for IT and information security are defined and filled.

Procedure Reconcile organisation chart, committee charters and job descriptions; note gaps and overlaps.

Evidence Organisation chart, committee charters, role descriptions

Audit steps 4 to 6

Step 04 DORA Art. 6(8)(b)

The organisation has defined how much IT risk it is prepared to bear, and this tolerance is aligned with its risk appetite.

Procedure Read the risk tolerance document and check whether thresholds are actually used in decisions and reports.

Evidence Risk tolerance statement, risk report with thresholds

Step 05 DORA Art. 6(8)(c)

Metrics are defined, measured and reported for IT and information security objectives.

Procedure Review the metrics catalogue and trace measurement method, data source and last reporting for three metrics.

Evidence Metrics catalogue, metrics report, data sources

Step 06 DORA Art. 5(2)(g)

Budget and resources for IT, security and skills are planned and reviewed regularly.

Procedure Review budget plan and actuals and check whether security and training needs are shown.

Evidence Budget plan, budget report, resource plan

Audit steps 7 to 9

Step 07

ISO/IEC 27001:2022 Annex A 5.1

A framework of policies is approved, communicated and reviewed at set intervals.

Procedure Analyse the policy register: approval, owners, date of last review.

Evidence Policy register, approval notes

Step 08

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

Members of management attend training on cyber risks regularly.

Procedure Request attendance records for management and check training content on risk assessment and impact.

Evidence Attendance records, training material

Step 09

DORA Art. 5(2)(i)

Management is informed regularly about major incidents, provider contracts and planned changes regarding critical providers.

Procedure Check reports to management for the last four quarters for this content.

Evidence Management reports, distribution lists, minutes

Audit steps 10 to 12

Step 10 — DORA Art. 6(8)(d)

A target architecture is described, and investments and projects are aligned with it.

Procedure Compare target architecture and project portfolio and trace the justification for three initiatives.

Evidence Target architecture, project portfolio, decision papers

Step 11 — ISO/IEC 27001:2022 Annex A 5.35; DORA Art. 6(6)

Governance of IT and information security is reviewed independently, for example by internal audit.

Procedure Review the audit plan and reports of the last two years and follow up the status of actions.

Evidence Audit plan, audit reports, action tracking

Step 12 — ISO/IEC 27001:2022 Annex A 5.3

Incompatible duties, such as operating and controlling the same systems, are segregated.

Procedure Check IT role design for conflicts and trace compensating controls for remaining conflicts.

Evidence Role descriptions, conflict matrix, evidence of compensating controls

Document request list

Request these 8 documents before you start

1. IT strategy with approval and evidence of review
2. Organisation chart and charters of IT committees
3. Risk tolerance statement
4. Metrics catalogue and metrics reports
5. IT budget plan and budget report
6. Policy register
7. Reports to management for the last four quarters
8. Training records of management

TYPICAL FINDINGS

- The IT strategy is outdated or has never been approved by management.
- Management receives no regular reports on cyber risks.
- Metrics are defined but not measured or not reported.
- Risk tolerance is not described, decisions lack a yardstick.
- Members of management have not attended training on cyber risks.
- Policies are not reviewed, owners are not named.

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