Sample audit programme

Supplier management

12 audit steps · ISO 27001, 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 5.19 · NIS2 Directive Art. 21(2)(d) · § 30(2) no. 4 BSIG · NIS2 Directive Art. 21(3) · ISO/IEC 27001:2022 Annex A 5.20 · ISO/IEC 27001:2022 Annex A 5.21 · ISO/IEC 27001:2022 Annex A 5.19 and 5.15 · ISO/IEC 27001:2022 Annex A 5.22 · BSI DER.2.1 · ISO/IEC 27001:2022 Annex A 5.19 and 5.18 · NIS2 Directive Art. 20

Audit objective and scope

The audit assesses whether the organisation governs information security in its relationships with service providers and suppliers: from recording and classification through selection and contractual safeguards to monitoring performance, handling changes and termination. It also assesses whether supply chains and subcontractors are taken into account.

SCOPE

- Service providers and suppliers with access to the organisation's information, systems or premises, and IT suppliers of essential services
- Processes for selection, engagement, monitoring, change and termination
- Responsible functions in procurement, business units, information security and legal
- Out of scope: rules specific to financial entities under DORA and cloud use, which are covered in separate samples

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 5.19; NIS2 Directive Art. 21(2)(d)

A policy on information security in supplier relationships exists, is approved and sets requirements according to the classification of the provider.

Procedure Read the policy and check whether classification, roles and minimum requirements are defined.

Evidence Policy with approval record, classification scheme

Step 02 — ISO/IEC 27001:2022 Annex A 5.19; § 30(2) no. 4 BSIG

A complete inventory of service providers and suppliers with classification, contact person and contract data is maintained.

Procedure Compare the inventory with the accounts payable list and access rights of externals to find providers that are not recorded.

Evidence Provider inventory, accounts payable extract, list of external users

Step 03 — ISO/IEC 27001:2022 Annex A 5.19; NIS2 Directive Art. 21(3)

Before engagement, risks are assessed and providers are checked for suitability, including in terms of information security.

Procedure For five new providers of the last twelve months, review the assessment made before the contract was signed.

Evidence Risk assessments, questionnaires, certificates, decision notes

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 5.20

Contracts contain security requirements, rules on the handling of information, incident reporting duties, audit rights and consequences of breaches.

Procedure Review the contracts in the sample against a checklist and record missing provisions.

Evidence Contracts and annexes, completed checklist

Step 05 — ISO/IEC 27001:2022 Annex A 5.21; NIS2 Directive Art. 21(2)(d)

The supply chain is considered: subcontractors are known, approved and subject to equivalent requirements.

Procedure For three essential providers, ask about subcontractors and check approval and the passing on of requirements.

Evidence Lists of subcontractors, approvals, contract clauses

Step 06 — ISO/IEC 27001:2022 Annex A 5.19 and 5.15

Access by service providers is limited to what is necessary, approved individually, time-limited and logged.

Procedure Read external accounts and check approval, time limit and use in recent months for a sample.

Evidence Extract of external accounts, approvals, logs

Audit steps 7 to 9

Step 07 ISO/IEC 27001:2022 Annex A 5.22

Performance and security of providers are monitored regularly, for example through reports, certificates and audits on site or remotely.

Procedure Review the monitoring plan and the reports of the last twelve months for essential providers.

Evidence Monitoring plan, performance reports, audit reports, certificates

Step 08 ISO/IEC 27001:2022 Annex A 5.22

Findings from monitoring are tracked and clarified with the provider until resolved.

Procedure Review open and closed findings of the last twelve months and check deadlines and closure.

Evidence Action list, correspondence, meeting minutes

Step 09 ISO/IEC 27001:2022 Annex A 5.22

Changes to services and contracts are assessed before they take effect, including in terms of information security.

Procedure Review contract amendments and announced provider changes in the sample for an assessment.

Evidence Change notices, assessment notes

Audit steps 10 to 12

Step 10 — ISO/IEC 27001:2022 Annex A 5.20; BSI DER.2.1

Security incidents at providers are reported, recorded and taken into the organisation's own incident management.

Procedure Check whether provider incidents appear in the incident register and whether reporting paths are agreed.

Evidence Incident register, contact list, reporting paths in the contract

Step 11 — ISO/IEC 27001:2022 Annex A 5.19 and 5.18

When a relationship ends, access is withdrawn, information is returned or deleted and deletion is confirmed.

Procedure Select two terminated provider relationships and check withdrawal of access and return or deletion of data.

Evidence Termination record, deletion confirmation, extract of access

Step 12 — NIS2 Directive Art. 20

Management is informed about supply chain risks and about significant findings.

Procedure Review reports and minutes of the last twelve months for topics on supplier management.

Evidence Reports to executive management, meeting minutes

Document request list

Request these 8 documents before you start

1. Policy on information security in supplier relationships
2. Provider inventory with classification
3. Risk assessments and selection documents of the sample
4. Contracts with annexes on security and data processing
5. Lists of subcontractors
6. Monitoring plan, performance reports and audit reports
7. Extract of external accounts and access by service providers
8. Termination records and deletion confirmations

TYPICAL FINDINGS

- The provider inventory is incomplete; some providers with system access are missing.
- Selection is made on price and expertise, with no assessment of information security.
- Contracts contain no reporting duty for security incidents and no audit rights.
- Subcontractors are not known or not approved.
- Monitoring is limited to receiving reports, and findings are not followed up.
- Provider access remains in place after the end of the contract.

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