Sample audit programme

IT asset and configuration management

12 audit steps · ISO 27001, DORA, 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 5.9 · NIS2 Directive Art. 21(2)(i) · DORA Art. 8(4) · ISO/IEC 27001:2022 Annex A 5.12 · DORA Art. 8(1) and (4) · ISO/IEC 27001:2022 Annex A 8.9 · DORA Art. 8(6) · ISO/IEC 27001:2022 Annex A 8.32 · BSI NET.3.4 · ISO/IEC 27001:2022 Annex A 5.10 and 5.11 · ISO/IEC 27001:2022 Annex A 7.14 and 8.10 · BSI CON.6 · DORA Art. 8(5) · DORA Art. 8(7)

Audit objective and scope

The audit assesses whether the organisation keeps a complete and current inventory of its information assets and IT components, assigns an owner to each asset and documents criticality, configuration and dependencies in a traceable way. It also assesses whether inventory and configuration management are linked to the change process and whether retired devices are wiped securely.

SCOPE

- Servers, clients, network components, mobile devices, software and cloud resources of the organisation
- Inventory and configuration management database (CMDB), including the processes for maintenance and reconciliation
- Disposal, return and re-use of devices and storage media
- Out of scope: fixed asset accounting, unless it serves as a source for the inventory

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 5.9; NIS2 Directive Art. 21(2)(i)

A policy defines which assets are to be inventoried, who maintains the inventory and how often it is reviewed.

Procedure Read the policy, establish approval and currency, and compare the defined asset classes with actual practice.

Evidence Asset management policy with approval note, role description

Step 02 — ISO/IEC 27001:2022 Annex A 5.9; DORA Art. 8(4)

The inventory is complete and also covers devices at remote sites, mobile devices, network resources and cloud resources.

Procedure Sample in both directions: find ten devices on site in the inventory and have ten inventory entries evidenced physically or technically.

Evidence Inventory extract, reconciliation record of the sample

Step 03 — ISO/IEC 27001:2022 Annex A 5.9

Each asset has an accountable owner who knows its protection needs and use.

Procedure For the sample, check that an owner is recorded and ask three owners about their role.

Evidence Inventory extract with owner field, interview notes

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 5.12; DORA Art. 8(1) and (4)

Assets are classified by criticality and protection needs; critical assets are flagged.

Procedure Review the classification scheme and trace for five assets whether the classification is justified and current.

Evidence Classification scheme, protection needs assessment, inventory extract

Step 05 — ISO/IEC 27001:2022 Annex A 8.9; DORA Art. 8(4)

Configurations and dependencies between systems, services and business processes are mapped in configuration management.

Procedure For one essential business process, trace the dependency chain in the CMDB and confirm it with operations.

Evidence CMDB extract with relationships, architecture overview

Step 06 — DORA Art. 8(6); ISO/IEC 27001:2022 Annex A 8.32

Inventory and configuration management are updated promptly after changes and reviewed regularly.

Procedure Select five completed changes and check whether the CMDB shows the new state; review evidence of the last review.

Evidence Change tickets, CMDB change history, review record

Audit steps 7 to 9

Step 07 — BSI NET.3.4

Unknown devices on the network are detected automatically, reconciled with the inventory and resolved.

Procedure Have the network discovery explained and check the deviation list of the last three months for follow-up.

Evidence Discovery tool reports, deviation list with resolution notes

Step 08 — ISO/IEC 27001:2022 Annex A 8.9

Documented security configurations exist for each system class, and compliance with them is monitored.

Procedure Read the configuration baselines for two system classes and analyse reports on deviations from the baseline.

Evidence Configuration baselines, compliance reports from configuration monitoring

Step 09 — ISO/IEC 27001:2022 Annex A 5.10 and 5.11

Rules for acceptable use are known, and assets are returned on leaving or changing role.

Procedure For five leavers in the last six months, trace the return of the assigned devices.

Evidence Acceptable use policy, leaver checklists, return records

Audit steps 10 to 12

Step 10 — ISO/IEC 27001:2022 Annex A 7.14 and 8.10; BSI CON.6

Retired devices and storage media are demonstrably wiped or destroyed before disposal or re-use.

Procedure Review the disposal process and request wiping or destruction evidence for five retired devices.

Evidence Disposal list, wiping logs, destruction certificates from the service provider

Step 11 — DORA Art. 8(5)

Dependencies on ICT third-party providers are recorded, especially for critical or important functions.

Procedure Check whether the CMDB or the provider register shows which assets depend on which provider.

Evidence Provider register, links between services and providers in the CMDB

Step 12 — DORA Art. 8(7)

Legacy systems are flagged as such, and their risks are assessed regularly.

Procedure Request the list of legacy systems and review the last risk assessment and the planned measures.

Evidence List of legacy systems, risk assessment, replacement plan

Document request list

Request these 8 documents before you start

1. Asset and configuration management policy
2. Current inventory extract with owner and classification
3. Classification scheme and protection needs assessment
4. CMDB extract with relationships for one essential business process
5. Network discovery reports and deviation list
6. Configuration baselines per system class
7. Disposal list with wiping and destruction evidence
8. List of legacy systems with risk assessment

TYPICAL FINDINGS

- Several inventories are kept in parallel and contradict each other.
- Cloud resources and mobile devices are missing from the inventory.
- Owners are not recorded or have left the organisation.
- The CMDB does not map dependencies and is not maintained after changes.
- There is no wiping evidence for retired storage media.
- Legacy systems are known, but their risks have never been assessed.

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