Sample audit programme

Software asset management

12 audit steps · ISO 27001, BSI

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

ISO/IEC 27001:2022 Annex A 5.32 · ISO/IEC 27001:2022 Annex A 5.9 · BSI APP.6 · ISO/IEC 27001:2022 Annex A 8.19 · ISO/IEC 27001:2022 Annex A 5.11 · ISO/IEC 27001:2022 Annex A 8.8

Audit objective and scope

The audit assesses whether the organisation keeps its use of software and cloud subscriptions in line with its acquired rights: through clear responsibilities, a complete inventory, evidenced entitlements and regular reconciliation. It also assesses whether procurement and installation are controlled and whether licences are reclaimed when no longer used.

SCOPE

- Software installed on clients and servers and software in virtualised environments
- Cloud subscriptions and user-based licences
- Contracts, proofs of entitlement and the software procurement process
- Out of scope: the contractual legal assessment of individual licence terms

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 5.32

A policy governs responsibility, procurement, use and proof of software licences.

Procedure Read the policy and ask the named owners about processes and tools.

Evidence Licence management policy, role description

Step 02 — ISO/IEC 27001:2022 Annex A 5.9; BSI APP.6

A complete inventory shows installed and used software, including cloud subscriptions.

Procedure Ask about the inventory data sources and compare coverage with the number of devices and accounts.

Evidence Software inventory, discovery tool coverage report

Step 03 — ISO/IEC 27001:2022 Annex A 5.32

Entitlements, with contracts, invoices and licence keys, are evidenced centrally and completely.

Procedure For five vendors, reconcile entitlements with proofs of purchase.

Evidence Licence register, contracts, invoices

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 5.32

Entitlements and usage are compared regularly; under- and over-licensing are corrected.

Procedure Review the last licence position for the main vendors and trace the handling of shortfalls.

Evidence Licence positions, action list

Step 05 — BSI APP.6

Software is procured only through a defined process that includes licence needs and approval.

Procedure Trace five purchases in the last twelve months from request to licence registration.

Evidence Purchase requests, approvals, licence register entries

Step 06 — ISO/IEC 27001:2022 Annex A 8.19

Users cannot install software on their own; installations follow approved channels.

Procedure Check technical restrictions on clients and search the inventory for unapproved software.

Evidence Software distribution configuration, list of unapproved software

Audit steps 7 to 9

Step 07 — ISO/IEC 27001:2022 Annex A 5.32

Licence metrics for virtualisation, servers and cloud are applied correctly.

Procedure For one vendor with core- or host-based metrics, trace the calculation.

Evidence Licence position calculation, infrastructure overview

Step 08 — ISO/IEC 27001:2022 Annex A 5.32

Licence terms of free and open source software are checked before use.

Procedure Review the approval process for freely available software and trace the check for three components.

Evidence Approval process, licence checks, component list

Step 09 — ISO/IEC 27001:2022 Annex A 5.32

The organisation is prepared for vendor audits: responsibility, procedure and data provision are defined.

Procedure Ask about the vendor audit procedure and review results of past audits including back payments.

Evidence Procedure description, reports of past audits

Audit steps 10 to 12

Step 10 — ISO/IEC 27001:2022 Annex A 5.11

Licences are reclaimed on leaving, role change or lack of use.

Procedure Analyse assigned subscriptions unused for 90 days and check reclamation for five leavers.

Evidence Subscription usage report, leaver checklists

Step 11 — BSI APP.6; ISO/IEC 27001:2022 Annex A 8.8

Software without vendor support is identified and replaced or treated as a risk.

Procedure Review the list of software whose support has ended and check replacement plans.

Evidence List of end-of-support software, replacement plans, risk acceptances

Step 12 — Good practice

Management receives regular reports on licence risks, costs and savings.

Procedure Check reports of the last twelve months for content and actions.

Evidence Licence management reports

Document request list

Request these 8 documents before you start

1. Licence management policy
2. Software inventory with coverage report
3. Licence register with contracts and proofs of purchase
4. Licence positions for the main vendors
5. Purchase requests and approvals of the last twelve months
6. Cloud subscription usage reports
7. List of end-of-support software
8. Reports of past vendor audits

TYPICAL FINDINGS

- Proofs of purchase for older licences can no longer be found.
- The licence position is only prepared when a vendor audit is announced.
- Users install software themselves, the inventory has gaps.
- Licence metrics for virtualised servers are calculated incorrectly.
- Subscriptions of former employees continue to be paid.
- End-of-support software runs without replacement plan or risk assessment.

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