Sample audit programme

Endpoint and mobile device security

12 audit steps · BSI, ISO 27001

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

ISO/IEC 27001:2022 Annex A 8.1 · BSI SYS.2.1 · BSI SYS.3.2.2 · ISO/IEC 27001:2022 Annex A 8.9 · ISO/IEC 27001:2022 Annex A 8.7 · BSI OPS.1.1.4 · ISO/IEC 27001:2022 Annex A 8.8 · BSI SYS.3.1 · ISO/IEC 27001:2022 Annex A 8.24 · BSI SYS.3.2.1 · ISO/IEC 27001:2022 Annex A 8.2 and 8.19 · ISO/IEC 27001:2022 Annex A 7.10 · BSI SYS.4.5 · ISO/IEC 27001:2022 Annex A 6.8 · ISO/IEC 27001:2022 Annex A 5.11 and 7.14

Audit objective and scope

The audit assesses whether the organisation controls its endpoints across their whole life cycle: from commissioning with a hardened baseline configuration through malware protection, updating and encryption to return and wiping. For mobile devices it assesses whether a mobile device management solution enforces the requirements effectively.

SCOPE

- Desktops and laptops running the operating systems in use
- Company smartphones and tablets, and private devices where used for work
- Tools for software distribution, malware protection and mobile device management
- Out of scope: servers and network components, which have their own audit programmes

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 8.1; BSI SYS.2.1

A policy governs procurement, configuration, use and return of endpoints, including mobile devices.

Procedure Read the policy, check approval and compare it with the device types actually in use.

Evidence Endpoint policy with approval, overview of device types

Step 02 — ISO/IEC 27001:2022 Annex A 8.1; BSI SYS.3.2.2

Only managed and registered devices gain access to company data.

Procedure Review access rules for email and file storage and trace whether unregistered devices are rejected.

Evidence Access rule configuration, list of registered devices

Step 03 — BSI SYS.2.1; ISO/IEC 27001:2022 Annex A 8.9

Endpoints are rolled out with a hardened baseline configuration; deviations are detected.

Procedure Review the baseline and read key settings such as firewall, screen lock and autostart on five devices.

Evidence Baseline configuration, group policies or profiles, readout of the sample

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 8.7; BSI OPS.1.1.4

Malware protection is active and current on all devices and reports detections centrally.

Procedure Analyse the central console: coverage, signature status and devices that have not reported in seven days.

Evidence Protection solution report on coverage and status, detection list

Step 05 — ISO/IEC 27001:2022 Annex A 8.8

Operating systems and applications are updated promptly; devices that are not updated are followed up.

Procedure Analyse the patch status of endpoints from the distribution tool and trace the handling of stragglers.

Evidence Patch report, list of outdated devices with actions

Step 06 — BSI SYS.3.1; ISO/IEC 27001:2022 Annex A 8.24

Storage on laptops and mobile devices is fully encrypted, and recovery keys are stored securely.

Procedure Retrieve the encryption status from the management console and check access to recovery keys.

Evidence Encryption report, permissions on the key store

Audit steps 7 to 9

Step 07

BSI SYS.3.2.2; BSI SYS.3.2.1

Mobile device management enforces requirements such as device lock, encryption and a minimum operating system version.

Procedure Review profiles and compliance rules in the MDM and trace non-compliant devices and their handling.

Evidence MDM profiles, compliance report, list of non-compliant devices

Step 08

BSI SYS.3.2.1; ISO/IEC 27001:2022 Annex A 8.1

Business and private data are separated on mobile devices; the use of private devices is governed.

Procedure Read the rule on private devices and have the technical separation (containers, app protection policies) demonstrated on a device.

Evidence Rule on private device use, app protection policy configuration

Step 09

ISO/IEC 27001:2022 Annex A 8.2 and 8.19

Local administrator rights are restricted; users can install software only through approved channels.

Procedure Read members of the local administrator groups on a sample and reconcile exceptions with their justification.

Evidence Readout of local groups, exception list with approvals

Audit steps 10 to 12

Step 10 — ISO/IEC 27001:2022 Annex A 7.10; BSI SYS.4.5

The use of removable media is governed and technically restricted.

Procedure Read the rule and check the technical block or allow list for removable media on one device.

Evidence Removable media rule, device control policy

Step 11 — BSI SYS.3.2.2; ISO/IEC 27001:2022 Annex A 6.8

Lost or stolen devices are reported without delay, locked and wiped remotely where needed.

Procedure For three loss reports in the last twelve months, trace report, lock and remote wipe with timestamps.

Evidence Loss reports, log of MDM actions, incident tickets

Step 12 — ISO/IEC 27001:2022 Annex A 5.11 and 7.14

On leaving or disposal, devices are taken back and wiped securely before re-use.

Procedure Select five leavers and trace the return and wiping of their devices.

Evidence Return records, wiping evidence

Document request list

Request these 8 documents before you start

1. Endpoint policy and rule on private devices
2. Baseline configuration per operating system
3. Malware protection report
4. Endpoint patch report
5. Encryption report
6. MDM profiles and compliance report
7. Exception list for local administrator rights
8. Loss reports and remote wipe log

TYPICAL FINDINGS

- Part of the fleet has not reported to the protection solution for weeks.
- Users have permanent local administrator rights without justification.
- Laptops are not consistently encrypted, recovery keys are stored unprotected.
- Private devices access email and files without registration.
- Lost devices are reported late and not wiped remotely.
- Returned devices are reissued without wiping evidence.

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