Sample audit programme

Remote access and mobile working

12 audit steps · BSI, 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 6.7 · BSI OPS.1.2.4 · BSI NET.3.3 · ISO/IEC 27001:2022 Annex A 8.20 · NIS2 Directive Art. 21(2)(j) · § 30(2) no. 10 BSIG · ISO/IEC 27001:2022 Annex A 8.5 · ISO/IEC 27001:2022 Annex A 8.1 · ISO/IEC 27001:2022 Annex A 8.8 · BSI TR-02102-3 · ISO/IEC 27001:2022 Annex A 8.22 · BSI OPS.1.2.5 · ISO/IEC 27001:2022 Annex A 8.15 and 8.16 · BSI INF.8 · BSI INF.9 · ISO/IEC 27001:2022 Annex A 7.7 · BSI CON.7 · ISO/IEC 27001:2022 Annex A 5.18

Audit objective and scope

The audit assesses whether the organisation handles remote access by staff and service providers through approved, hardened gateways with multi-factor sign-in and limits and monitors access to what is required. It also assesses whether rules for working from home, on the move and abroad exist and are followed.

SCOPE

- VPN, zero trust access, remote desktop gateways and comparable remote access
- Remote maintenance access by service providers
- Working from home, on the move and on trips abroad
- Out of scope: the general network architecture, which has its own audit programme

Audit steps 1 to 3

Step 01 ISO/IEC 27001:2022 Annex A 6.7; BSI OPS.1.2.4

A policy governs mobile working and teleworking, including permitted locations, devices and rules of conduct.

Procedure Read the policy, check approval and compare it with the agreement on mobile working.

Evidence Mobile working policy, agreement with employee representatives

Step 02 BSI NET.3.3; ISO/IEC 27001:2022 Annex A 8.20

Remote access is possible only through approved, centrally managed gateways.

Procedure Compare the overview of remote access gateways with a scan of services reachable from outside.

Evidence List of remote access gateways, external scan result

Step 03 NIS2 Directive Art. 21(2)(j); § 30(2) no. 10 BSIG; ISO/IEC 27001:2022 Annex A 8.5

Every remote access requires sign-in with multiple factors.

Procedure Check the sign-in configuration of the gateways and have accounts without a second factor listed.

Evidence Sign-in configuration, exception list

Audit steps 4 to 6

Step 04

ISO/IEC 27001:2022 Annex A 8.1

Only managed devices in a verified state may connect.

Procedure Review device posture rules and trace a connection attempt from an unmanaged device.

Evidence Device posture rules, log of rejected connections

Step 05

BSI NET.3.3; ISO/IEC 27001:2022 Annex A 8.8

VPN gateways and access systems are hardened and updated promptly.

Procedure Compare the version of the access systems with vendor advisories and trace the response to the last critical vulnerability.

Evidence Version status, patch log, vendor security advisories

Step 06

BSI TR-02102-3

The VPN tunnel uses recommended protocols and algorithms.

Procedure Read the configuration of protocol versions and encryption algorithms and compare it with the recommendations.

Evidence VPN configuration extract

Audit steps 7 to 9

Step 07 — ISO/IEC 27001:2022 Annex A 8.22

Remote access reaches only the networks and systems needed for the respective task.

Procedure Analyse access rules per user group and flag blanket access to the whole internal network.

Evidence Gateway rule set per group

Step 08 — BSI OPS.1.2.5

Remote maintenance by service providers takes place only after approval, time-limited and traceable.

Procedure Check five remote maintenance sessions for reason, approval, duration and log.

Evidence Remote maintenance logs, approvals, contract provisions

Step 09 — ISO/IEC 27001:2022 Annex A 8.15 and 8.16

Sign-ins and sessions over remote access are logged and monitored for anomalies.

Procedure Review monitoring rules for remote access, such as sign-ins from unusual countries, and trace one alert.

Evidence Log extract, rule catalogue, alert example

Audit steps 10 to 12

Step 10 — BSI INF.8; BSI INF.9; ISO/IEC 27001:2022 Annex A 7.7

Rules for the workplace at home and on the move protect information against viewing and loss.

Procedure Check rules on privacy screens, printouts and storage and ask five employees whether they know them.

Evidence Rules of conduct, interview notes

Step 11 — BSI CON.7

Special rules apply to travel and work abroad, for example on devices and taking data along.

Procedure Read the rule for trips abroad and trace its application for two trips.

Evidence Rule for trips abroad, travel devices, approvals

Step 12 — ISO/IEC 27001:2022 Annex A 5.18

Remote access permissions are reviewed regularly and revoked immediately on leaving.

Procedure Reconcile members of the access groups with headcount and review the last review.

Evidence Group members, leaver list, review record

Document request list

Request these 8 documents before you start

1. Mobile working and teleworking policy
2. List of remote access gateways and result of an external scan
3. Configuration of sign-in and device posture checks
4. Version status and patch log of the access systems
5. Gateway rule set per user group
6. Remote maintenance logs and contract provisions with service providers
7. Rule for trips abroad
8. Record of the last review of access permissions

TYPICAL FINDINGS

- An old remote access gateway is still reachable from outside and usable without a second factor.
- VPN gateways were not updated promptly after critical vendor advisories.
- The whole internal network is reachable through remote access.
- Remote maintenance access for service providers is permanently open.
- Private devices can connect without checks.
- Access permissions are never reviewed.

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