Sample audit programme

Network security and segmentation

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 8.20 · BSI NET.1.1 · ISO/IEC 27001:2022 Annex A 8.22 · BSI NET.3.2 · ISO/IEC 27001:2022 Annex A 8.32 · BSI NET.1.2 · ISO/IEC 27001:2022 Annex A 8.21 · § 30(2) no. 10 BSIG · ISO/IEC 27001:2022 Annex A 8.2 · ISO/IEC 27001:2022 Annex A 8.16 · NIS2 Directive Art. 21(2)(f)

Audit objective and scope

The audit assesses whether the organisation designs and delimits its networks by protection requirement, controls traffic between zones, runs network services and remote access securely and keeps changes and anomalies in the network under control. It also assesses whether documentation reflects the actual structure.

SCOPE

- Internal networks, data centre networks, site and remote connections, wireless networks and the gateways to the internet
- Firewalls, routers, switches, VPN gateways and network services such as DNS and DHCP
- Network management, changes to rules and monitoring of traffic
- Out of scope: application security and endpoint hardening, unless agreed separately

Audit steps 1 to 3

Step 01

ISO/IEC 27001:2022 Annex A 8.20; BSI NET.1.1

A network security policy exists, is approved and governs the design, operation and access to networks.

Procedure Read the policy, establish approval and currency and compare it with the network documentation.

Evidence Policy with approval record, network documentation

Step 02

BSI NET.1.1; ISO/IEC 27001:2022 Annex A 8.20

Network diagrams and the zone model are current and reflect the actual structure, including the connections to providers and cloud links.

Procedure Compare the network diagram with the configuration of routers and firewalls at three sites or zones.

Evidence Network diagrams, zone model, configuration extracts

Step 03

ISO/IEC 27001:2022 Annex A 8.22; BSI NET.1.1

Networks are separated into zones by protection requirement; essential systems and management networks sit in their own segments.

Procedure Compare the zone concept with the implementation and test from a user network whether management interfaces are reachable.

Evidence Segmentation concept, reachability test results, configuration extracts

Audit steps 4 to 6

Step 04

BSI NET.3.2; ISO/IEC 27001:2022 Annex A 8.20

Traffic between zones is controlled by firewalls, and the default rule denies whatever is not expressly allowed.

Procedure Review the rule sets of the firewalls between internet, user network and data centre and check the default rule.

Evidence Rule set extracts, configuration of the default rule

Step 05

BSI NET.3.2

Rules are justified, have owners and are reviewed regularly for necessity; overly broad and unused rules are removed.

Procedure Select ten rules, check justification and owners and compare with hit counts of recent months.

Evidence Rule set with comments, report of the last rule review, hit statistics

Step 06

ISO/IEC 27001:2022 Annex A 8.32; BSI NET.1.2

Changes to network components and rules go through an approved change procedure and are documented.

Procedure Compare changes to firewall rules of the last six months with the change requests.

Evidence Firewall change logs, change requests

Audit steps 7 to 9

Step 07 — ISO/IEC 27001:2022 Annex A 8.21

Network services, including those provided by service providers, are defined with security features, service levels and management requirements and are monitored.

Procedure Read agreements on network services and trace compliance with the security features for two services.

Evidence Agreements on network services, performance reports

Step 08 — ISO/IEC 27001:2022 Annex A 8.20; § 30(2) no. 10 BSIG

Remote access is limited to what is necessary, encrypted and secured by multi-factor authentication.

Procedure Check the configuration of VPN gateways and remote maintenance access and go through the exceptions.

Evidence Configuration extracts, exception list with approval

Step 09 — BSI NET.1.2; ISO/IEC 27001:2022 Annex A 8.2

Management access to network components is secured: separate management networks, individual accounts, no default passwords, unneeded services disabled.

Procedure Select ten network components and check accounts, enabled services and access paths.

Evidence Configuration extracts, account list of network components

Audit steps 10 to 12

Step 10

ISO/IEC 27001:2022 Annex A 8.22

Wireless networks are secured against unauthorised access and separated from internal networks; guest access has no access to internal systems.

Procedure Check the configuration of wireless networks and guest access and evidence the separation with a test.

Evidence Configuration extracts, test result

Step 11

ISO/IEC 27001:2022 Annex A 8.16; BSI NET.1.1

Traffic and network events are monitored, and unusual connections generate alerts that are followed up.

Procedure Check monitoring of the gateways to the internet and between zones and follow up three alerts.

Evidence Monitoring configuration, alert list, tickets

Step 12

NIS2 Directive Art. 21(2)(f)

The effectiveness of separation is checked regularly through security tests of the networks, and findings are corrected.

Procedure Review reports of the latest network tests and check whether findings were corrected.

Evidence Test reports, action list

Document request list

Request these 8 documents before you start

1. Network security policy
2. Network diagrams and zone model
3. Segmentation concept
4. Firewall rule set extracts with justifications
5. Report of the last rule review
6. Firewall change logs and change requests
7. Configuration extracts of VPN gateways and network components
8. Network test reports

TYPICAL FINDINGS

- The network diagram deviates from reality, and connections to providers are not documented.
- User networks can reach management interfaces of servers and network components.
- Firewall rules have not been reviewed for years; very broad rules exist without justification.
- Changes to firewall rules are made without a change request.
- Default accounts or default passwords are active on network components.
- Guest access is not effectively separated from internal networks.

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