Sample audit programme

NIS2

Access management

13 audit steps · NIS2

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

NIS2 Directive Art. 21(2)(i) · BSI ORP.4 · NIS2 Directive Art. 20 · ISO/IEC 27001:2022 Annex A 5.15 · ISO/IEC 27001:2022 Annex A 5.16 · ISO/IEC 27001:2022 Annex A 5.18 · ISO/IEC 27001:2022 Annex A 8.2 · 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 5.17 and 8.5 · ISO/IEC 27001:2022 Annex A 8.15

Audit objective and scope

The audit assesses whether the organisation controls access to network and information systems through a documented and effective procedure: from the request through approval and provisioning to regular review and withdrawal. It also assesses whether elevated rights and remote access are additionally protected.

SCOPE

- Business applications, operating systems, databases, network components and administration consoles used for essential services or processes
- User accounts of employees, externals and service providers, as well as technical and emergency accounts
- Joiner, mover and leaver processes together with the HR department
- Out of scope: physical access and the authentication of customer accounts, unless agreed separately

Audit steps 1 to 3

Step 01

NIS2 Directive Art. 21(2)(i); BSI ORP.4

An access control policy exists, is approved by management, is current and covers the systems, data and locations in scope.

Procedure Read the policy, establish approval, version and date of the last review, and compare its scope with the system overview.

Evidence Policy with approval record and change history, system overview

Step 02

NIS2 Directive Art. 20

Management is informed about access risks and supports the risk management measures.

Procedure Review reports and minutes of the last twelve months for topics on access and authorisations.

Evidence Reports to executive management, meeting minutes, decisions

Step 03

BSI ORP.4; ISO/IEC 27001:2022 Annex A 5.15

A role and authorisation concept defines which role receives which rights and follows the principle of least privilege.

Procedure For five selected applications, compare the concept with the rights actually granted and ask about deviations.

Evidence Role matrix, authorisation concepts per application, system extracts of rights

Audit steps 4 to 6

Step 04 — BSI ORP.4

Owners are named for systems and roles and approve authorisations before they are granted.

Procedure Select ten access requests and check whether the responsible business owner approved them before provisioning.

Evidence Requests or tickets with approval and timestamp, list of owners

Step 05 — BSI ORP.4; ISO/IEC 27001:2022 Annex A 5.16

New accounts and rights for joiners match the request and the role.

Procedure Draw a sample from the HR joiner list and compare the rights granted with the request.

Evidence Joiner list, requests, extract of granted rights

Step 06 — BSI ORP.4; ISO/IEC 27001:2022 Annex A 5.18

When a person changes role, rights that are no longer needed are withdrawn.

Procedure Select role changes from the last twelve months and compare rights before and after the change.

Evidence List of changes, rights extracts before and after, tickets

Audit steps 7 to 9

Step 07

BSI ORP.4; ISO/IEC 27001:2022 Annex A 5.18

Accounts of departed people are disabled promptly.

Procedure Compare the leaver list at a cut-off date with active accounts and determine the time between departure and deactivation.

Evidence Leaver list, account list with status and deactivation date, deactivation log

Step 08

BSI ORP.4; ISO/IEC 27001:2022 Annex A 5.18

Authorisations are reviewed by their owners at defined intervals and findings are followed up.

Procedure Review the latest recertification: scope, response rate, deadlines and whether revoked rights were actually removed.

Evidence Recertification reports, confirmations by owners, tickets for removal

Step 09

BSI ORP.4; ISO/IEC 27001:2022 Annex A 8.2

Privileged accounts are inventoried, limited to what is necessary and separated from day-to-day work.

Procedure Extract privileged accounts directly from the systems, compare them with the inventory and check whether administrator accounts are used for email or internet access.

Evidence Inventory of privileged accounts, system extracts of administrator groups, approvals

Audit steps 10 to 13

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

Multi-factor authentication is used for remote access and privileged access; exceptions are justified and approved.

Procedure Check the configuration of VPN, remote access and administration consoles and go through the exceptions with their justification.

Evidence Configuration extracts, list of exceptions with approval

Step 11 BSI ORP.4

Technical, service and emergency accounts are recorded, have a responsible person and a defined password procedure.

Procedure Derive service and emergency accounts from the systems and, for a sample, ask for the owner and the password procedure.

Evidence Inventory of technical accounts, procedure description, evidence of password change

Step 12 ISO/IEC 27001:2022 Annex A 5.17 and 8.5

Requirements for passwords and other authentication factors are defined and technically enforced.

Procedure Compare the defined rules with the settings in the directory service and central applications.

Evidence Policy, configuration extracts

Step 13 ISO/IEC 27001:2022 Annex A 8.15

Changes to authorisations and the use of privileged accounts are logged and reviewed.

Procedure Check logging for privileged activity and trace a review together with the response to a finding.

Evidence Log configuration, review results, alerts and tickets

Document request list

Request these 8 documents before you start

1. Access control and authorisation policy
2. Role and authorisation concepts, role matrix
3. Inventory of systems and of privileged and technical accounts
4. HR joiner and leaver lists for the last twelve months
5. Reports of the latest recertification with follow-up
6. System extracts of users, groups and administrator rights at a cut-off date
7. Configuration evidence for multi-factor authentication and password rules
8. Reports to executive management on access topics

TYPICAL FINDINGS

> The review of authorisations does not take place, or is confirmed without checking the details.

> Accounts of departed people stay active for weeks because the notification from HR is missing.

> Privileged accounts are not fully inventoried; some administrators use their account for everyday work.

> Service accounts have no responsible person and a password that has not changed for years.

> Multi-factor authentication applies with unjustified exceptions, in particular for service providers.

> Roles are not documented; rights are granted by copying existing users.

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