Sample audit programme

# Privileged access

## 12 audit steps · NIS2, ISO 27001, BSI

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

NIS2 Directive Art. 21(2)(i) · ISO/IEC 27001:2022 Annex A 8.2 · BSI ORP.4 · ISO/IEC 27001:2022 Annex A 8.2 and 5.15 · NIS2 Directive Art. 21(2)(j) · § 30(2) no. 10 BSIG · ISO/IEC 27001:2022 Annex A 8.15 and 8.2 · ISO/IEC 27001:2022 Annex A 5.18 and 8.2 · ISO/IEC 27001:2022 Annex A 5.19 and 8.2 · ISO/IEC 27001:2022 Annex A 5.18

## Audit objective and scope

The audit assesses whether the organisation controls privileged access deliberately: inventory and accountability, restriction to what is necessary, additional authentication, protected storage of credentials, logging of use and regular review. It also assesses whether emergency access and access by service providers are regulated.

### SCOPE

- Administrator accounts for operating systems, databases, directory services, network components, virtualisation and cloud consoles
- Technical accounts, service accounts and emergency accounts with elevated rights
- Access by service providers with privileged rights
- Out of scope: general access management for ordinary users, which is covered in a separate sample

## Audit steps 1 to 3

Step 01 — NIS2 Directive Art. 21(2)(i); ISO/IEC 27001:2022 Annex A 8.2

### A policy governs the granting, use and withdrawal of privileged rights and is approved by management.

**Procedure** Read the policy, establish approval and currency, and compare its scope with the system overview.

**Evidence** Policy with approval record, system overview

Step 02 — ISO/IEC 27001:2022 Annex A 8.2; BSI ORP.4

### All privileged accounts are inventoried, and each account is assigned a responsible person and a purpose.

**Procedure** Read privileged accounts directly from five systems and compare them with the inventory.

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

Step 03 — ISO/IEC 27001:2022 Annex A 8.2 and 5.15

### Privileged rights are limited to what is necessary; roles are justified by the business and approved.

**Procedure** Select ten privileged accounts and check justification and approval of the rights.

**Evidence** Requests and approvals, role descriptions

## Audit steps 4 to 6

**Step 04** BSI ORP.4; ISO/IEC 27001:2022 Annex A 8.2

### Administrators use an account without elevated rights for daily work and a separate account for administrative tasks.

**Procedure** Check whether administrator accounts have a mailbox or are used for internet access.

**Evidence** Account list with mailbox, analysis of internet use by privileged accounts

**Step 05** NIS2 Directive Art. 21(2)(j); § 30(2) no. 10 BSIG

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

**Procedure** Check configuration of administration consoles, VPN and cloud access and go through the exceptions.

**Evidence** Configuration extracts, list of exceptions with approval

**Step 06** ISO/IEC 27001:2022 Annex A 8.2; BSI ORP.4

### Credentials of privileged accounts, in particular service and emergency accounts, are kept in a protected vault or equivalent and are changed after use or at defined intervals.

**Procedure** Have the safekeeping procedure described and check the date of the last change for a sample.

**Evidence** Procedure description, vault extract, evidence of changes

## Audit steps 7 to 9

Step 07 — ISO/IEC 27001:2022 Annex A 8.15 and 8.2

### Administrative activity and use of privileged accounts are logged; sessions are recorded on particularly critical systems.

**Procedure** Check logging for two critical systems and trace an administrative activity from the log.

**Evidence** Logging configuration, log extracts, recordings

Step 08 — ISO/IEC 27001:2022 Annex A 5.18 and 8.2

### Privileged rights are reviewed at defined intervals by their owners, and findings are implemented.

**Procedure** Review the last review: scope, response rate, deadlines and actual withdrawal of rights no longer needed.

**Evidence** Review reports, confirmations, tickets for withdrawal

Step 09 — ISO/IEC 27001:2022 Annex A 8.2

### Where needed, elevated rights are granted for a limited time and withdrawn automatically afterwards where the technology allows.

**Procedure** Check whether time-limited rights are in use and examine a sample of grants for withdrawal after expiry.

**Evidence** Configuration of time-limited grants, log of granting and withdrawal

## Audit steps 10 to 12

**Step 10** ISO/IEC 27001:2022 Annex A 8.2; BSI ORP.4

### Emergency access is regulated: triggering, approval, use, logging and subsequent review.

**Procedure** Review all uses of emergency accounts in the last twelve months and check approval and subsequent review.

**Evidence** Emergency access procedure, list of uses, evidence of review

**Step 11** ISO/IEC 27001:2022 Annex A 5.19 and 8.2

### Privileged access by service providers is regulated by contract, approved individually, time-limited and logged.

**Procedure** Check access of three service providers: approval, time limit, authentication and logs of the latest sessions.

**Evidence** Contracts, approvals, access logs

**Step 12** ISO/IEC 27001:2022 Annex A 5.18; BSI ORP.4

### Accounts of departed or transferred administrators are blocked or adjusted promptly.

**Procedure** Compare leaver and mover lists with the administrator groups and determine the time until adjustment.

**Evidence** Leaver list, extract of administrator groups, blocking record

Document request list

# Request these 8 documents before you start

1. Policy on privileged access
2. Inventory of privileged, technical and emergency accounts
3. System extracts of administrator groups on a reference date
4. Configuration evidence of multi-factor authentication
5. Procedure description for the safekeeping of credentials
6. Log extracts of administrative activity
7. Reports of the last review of privileged rights
8. Contracts and approvals for access by service providers

## TYPICAL FINDINGS

There is no complete overview of privileged accounts; service accounts have no responsible person.

Administrators work daily with their privileged account, including for e-mail and internet.

Credentials of emergency and service accounts sit in spreadsheets or have been unchanged for years.

Multi-factor authentication is not required consistently for administrators, and exceptions are not justified.

The review of privileged rights is confirmed without any rights actually being withdrawn.

Service providers keep access after the end of the engagement.

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