Sample audit programme

Active Directory and Entra ID

13 audit steps · BSI, ISO 27001, BSIG

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

BSI APP.2.1 · BSI APP.2.2 · ISO/IEC 27001:2022 Annex A 8.2 · § 30(2) no. 10 BSIG · ISO/IEC 27001:2022 Annex A 8.5 · ISO/IEC 27001:2022 Annex A 5.16 and 5.18 · BSI ORP.4 · ISO/IEC 27001:2022 Annex A 5.17 · ISO/IEC 27001:2022 Annex A 5.16 · ISO/IEC 27001:2022 Annex A 5.18 · ISO/IEC 27001:2022 Annex A 8.15 and 8.16 · ISO/IEC 27001:2022 Annex A 8.13

Audit objective and scope

The audit assesses whether Active Directory and Entra ID are operated under a clear administration model, whether highly privileged groups and accounts are minimal and monitored and whether sign-in methods, service accounts, guest access and synchronisation between both directories are set up securely. It also assesses whether the directory service can be recovered after a compromise.

SCOPE

- On-premises Active Directory with all domains and domain controllers
- Entra ID tenant including conditional access, guest accounts and application registrations
- Synchronisation between the on-premises directory and Entra ID
- Out of scope: permissions within individual business applications

Audit steps 1 to 3

Step 01 — BSI APP.2.1; BSI APP.2.2

Responsibility and the operating concept for the directory services are documented and current.

Procedure Read the operating concept and compare it with the actual domain and tenant structure.

Evidence Operating concept, overview of domains and trusts

Step 02 — BSI APP.2.2; ISO/IEC 27001:2022 Annex A 8.2

A tiered administration model separates administration of the directory services from administration of servers and workstations.

Procedure Have the model explained and check whether domain administrators sign in only on designated systems.

Evidence Administration model description, logon restrictions, sign-in logs

Step 03 — ISO/IEC 27001:2022 Annex A 8.2; BSI APP.2.2

Highly privileged groups and roles have few, personally assigned members and are reviewed regularly.

Procedure Read members of highly privileged groups and Entra roles and reconcile them with approved assignments.

Evidence Readout of groups and roles, approvals, recertification record

Audit steps 4 to 6

Step 04 § 30(2) no. 10 BSIG; ISO/IEC 27001:2022 Annex A 8.5

Administrative sign-ins and remote access are protected with multiple factors; conditional access rules have no unreviewed gaps.

Procedure Analyse conditional access rules, list exceptions and check factor registration status.

Evidence Export of conditional access rules, exception list, registration report

Step 05 ISO/IEC 27001:2022 Annex A 8.2

Emergency access accounts are set up, stored securely, monitored and tested.

Procedure Check number, storage and monitoring of emergency access accounts and review the last test.

Evidence Emergency access rule, alert rule for sign-ins, test record

Step 06 ISO/IEC 27001:2022 Annex A 5.16 and 5.18; BSI ORP.4

Accounts are adjusted promptly for joiners, movers and leavers; inactive accounts are disabled.

Procedure Read accounts without sign-in for 90 days and check five leavers for prompt disabling.

Evidence List of inactive accounts, leaver notifications, disabling times

Audit steps 7 to 9

Step 07

ISO/IEC 27001:2022 Annex A 5.17; BSI APP.2.2

Service accounts have owners, only necessary rights and strong, rotated or managed passwords.

Procedure Read service accounts, flag privileged ones and check password age and owners.

Evidence List of service accounts with owners, password age, rights

Step 08

ISO/IEC 27001:2022 Annex A 8.5; BSI APP.2.2

Password rules are adequate, and legacy authentication protocols and encryption types are disabled.

Procedure Read password policies and settings for legacy protocols; review results of a directory assessment tool.

Evidence Policy extract, assessment tool report

Step 09

ISO/IEC 27001:2022 Annex A 8.2

The server synchronising the on-premises directory with Entra ID is protected like a domain controller.

Procedure Check administration, network access and permissions of the synchronisation server and its service accounts.

Evidence System documentation, members of local administrators, rights of the synchronisation account

Audit steps 10 to 13

Step 10 — ISO/IEC 27001:2022 Annex A 5.16

Guest accounts and external identities are approved, time-limited and reviewed regularly.

Procedure Read guest accounts, flag the oldest and inactive guests and trace the review process.

Evidence List of guest accounts, invitation settings, review evidence

Step 11 — ISO/IEC 27001:2022 Annex A 5.18

Application registrations and granted consents are controlled; users cannot grant applications far-reaching permissions.

Procedure Check user consent settings and list applications with high permissions.

Evidence Consent settings, list of applications with permissions

Step 12 — ISO/IEC 27001:2022 Annex A 8.15 and 8.16; BSI APP.2.2

Sign-ins and changes to directory objects are logged, analysed centrally and alerted on when anomalous.

Procedure Review monitoring rules for changes to privileged groups and trace one alert.

Evidence Monitoring policy, rule catalogue, alert example

Step 13 — ISO/IEC 27001:2022 Annex A 8.13; BSI APP.2.2

Recovery of the directory service after compromise is planned, backed up and tested.

Procedure Read the recovery plan, check domain controller backups and review the last recovery test.

Evidence Recovery plan, backup evidence, test record

Document request list

Request these 8 documents before you start

1. Operating concept of the directory services and administration model
2. Readout of privileged groups and Entra roles
3. Export of conditional access rules with exceptions
4. Rule on emergency access accounts
5. List of service accounts with owners
6. List of guest accounts and applications with permissions
7. Report of a directory assessment tool
8. Recovery plan and test record

TYPICAL FINDINGS

- Domain administrators sign in on ordinary workstations.
- Highly privileged groups contain service accounts and former employees.
- Exceptions from the second factor are broad and not time-limited.
- Service accounts have had unchanged passwords and administrator rights for years.
- Guest accounts remain active after projects end.
- Recovery of the directory service has never been rehearsed.

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