Sample audit programme

SAP authorisations

13 audit steps · BSI, ISO 27001, GoBD

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

BSI APP.4.2 · ISO/IEC 27001:2022 Annex A 5.15 · ISO/IEC 27001:2022 Annex A 5.18 · ISO/IEC 27001:2022 Annex A 5.3 · GoBD para. 100 · ISO/IEC 27001:2022 Annex A 8.2 · ISO/IEC 27001:2022 Annex A 8.2 and 8.15 · GoBD para. 107 · ISO/IEC 27001:2022 Annex A 8.15 · ISO/IEC 27001:2022 Annex A 8.31 and 8.32 · BSI ORP.4

Audit objective and scope

The audit assesses whether the organisation grants authorisations in the ERP system according to an approved concept and reviews them regularly, whether incompatible functions are segregated and whether critical authorisations, standard and emergency users and changes to the production system are controlled and traceable. It also assesses whether logging secures the traceability of changes relevant to bookkeeping.

SCOPE

- Productive SAP systems and clients with processes relevant to bookkeeping
- Roles, users, request and approval process and the segregation of duties rule set
- Emergency users, standard users, interface and system users
- Out of scope: authorisations in upstream systems outside SAP, which have their own audits

Audit steps 1 to 3

Step 01

BSI APP.4.2; ISO/IEC 27001:2022 Annex A 5.15

An authorisation concept describes role design, naming conventions, granting, review and responsibilities and is approved.

Procedure Read the concept, check approval and trace naming conventions for ten roles in the system.

Evidence Authorisation concept with approval, role list

Step 02

BSI APP.4.2; ISO/IEC 27001:2022 Annex A 5.18

Roles are tailored to business tasks and have accountable role owners from the business.

Procedure Check content and owner for five roles and ask owners about their knowledge of the role content.

Evidence Role descriptions, list of role owners

Step 03

ISO/IEC 27001:2022 Annex A 5.18

Authorisations are granted only on request with approval by line manager and role owner.

Procedure Reconcile ten role assignments of the last six months with requests and approvals.

Evidence User master change documents, requests, approvals

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 5.3; GoBD para. 100

A segregation of duties rule set is defined; conflicts are detected, assessed and offset by controls.

Procedure Review the rule set, run a current conflict analysis and trace compensating controls for three conflicts.

Evidence Segregation of duties rule set, conflict report, control evidence

Step 05 — ISO/IEC 27001:2022 Annex A 8.2; BSI APP.4.2

Critical authorisations such as full access profiles, debugging with change rights or direct table maintenance are limited to few justified cases.

Procedure Analyse users with critical profiles and authorisations and reconcile them with approved exceptions.

Evidence Analysis of critical authorisations, exception approvals

Step 06 — BSI APP.4.2

Standard users are locked or secured with changed passwords and monitored in all clients.

Procedure Read status and password change of standard users in all clients.

Evidence Analysis of standard users per client

Audit steps 7 to 9

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

Emergency users are activated only when needed; their activities are logged and reviewed afterwards.

Procedure Select five emergency uses and trace reason, activation, log and follow-up review.

Evidence Emergency logs, approvals, evidence of follow-up review

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

Authorisations are recertified regularly by line managers and role owners; removals are implemented.

Procedure Check the last recertification for completeness and trace implementation in the system for five removals.

Evidence Recertification record, change documents

Step 09 — GoBD para. 107; BSI APP.4.2

Productive clients and the production system are locked against direct changes; openings are approved and logged.

Procedure Read system and client changeability settings and trace openings in the last twelve months.

Evidence System settings, system changeability log, approvals

Audit steps 10 to 13

Step 10 — GoBD para. 107; ISO/IEC 27001:2022 Annex A 8.15

Table logging and change documents are active for data relevant to bookkeeping.

Procedure Check system parameters for table logging and have logging evidenced for three relevant tables.

Evidence System parameters, table log analysis

Step 11 — ISO/IEC 27001:2022 Annex A 8.31 and 8.32

Development, test and production are separated; changes reach production only through the transport system.

Procedure Review transport routes and check whether development rights are granted in the production system.

Evidence Transport landscape, transport logs, analysis of development rights

Step 12 — BSI APP.4.2; ISO/IEC 27001:2022 Annex A 8.2

Interface and system users have only the rights needed for their task and cannot be used for dialogue sign-in.

Procedure Read users of type system and communication and check rights and user type.

Evidence List of technical users with roles and user type

Step 13 — ISO/IEC 27001:2022 Annex A 5.18; BSI ORP.4

Users of former employees are locked promptly and validity dates are maintained.

Procedure Reconcile the HR leaver list with active SAP users and their last sign-in.

Evidence Leaver list, user list with status and last sign-in

Document request list

Request these 8 documents before you start

1. Authorisation concept with approval
2. Role list with role owners
3. Segregation of duties rule set and current conflict analysis
4. Analysis of critical authorisations and standard users
5. Emergency user logs with follow-up review
6. Record of the last recertification
7. System changeability settings and log
8. List of technical users

TYPICAL FINDINGS

- Several users have full access profiles in the production system.
- Segregation of duties conflicts are known, compensating controls are missing.
- Emergency users are used, but their logs are never reviewed.
- The production system was open for direct changes for weeks.
- Table logging is not activated.
- Former employees still have valid 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