Sample audit programme

Change management

13 audit steps · BSI, ISO 27001

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

BSI OPS.1.1.3 · ISO/IEC 27001:2022 Annex A 8.32 · ISO/IEC 27001:2022 Annex A 8.31 · ISO/IEC 27001:2022 Annex A 8.9 · ISO/IEC 27001:2022 Annex A 8.2

Audit objective and scope

The audit assesses whether changes to productive IT systems are made in a controlled way: with a request, an assessment of impact, approval before implementation, a test, a rollback plan and documentation. It also assesses whether all changes actually go through the procedure.

SCOPE

- Changes to applications, infrastructure, configurations and network components in production
- Standard changes, normal changes and emergency changes
- Roles in the procedure, such as requester, approver and implementer, and the development, test and production environments
- Out of scope: the methodology of software development itself, unless agreed separately

Audit steps 1 to 3

Step 01 — BSI OPS.1.1.3; ISO/IEC 27001:2022 Annex A 8.32

A change process exists, is approved and distinguishes standard, normal and emergency changes.

Procedure Read the process description and check whether categories, roles and flows are defined for each category.

Evidence Process description with approval, catalogue of standard changes

Step 02 — BSI OPS.1.1.3

Every change is requested with a description, justification, affected systems and rollback plan.

Procedure Select ten changes from the last six months and check the requests for completeness.

Evidence Change requests or tickets

Step 03 — ISO/IEC 27001:2022 Annex A 8.32

Impact and risks, including for information security, are assessed before approval.

Procedure In the sample, check whether and how impact and security aspects were assessed.

Evidence Assessment notes, risk rating in the ticket

Audit steps 4 to 6

Step 04

ISO/IEC 27001:2022 Annex A 8.32

Changes are approved by an authorised body before implementation.

Procedure Compare the time of approval with the time of implementation and check the authority of the approvers.

Evidence Approvals with timestamp, list of authorities, minutes of the change board

Step 05

ISO/IEC 27001:2022 Annex A 8.31

Requester, approver and implementer are separated, and development, test and production are separated from each other.

Procedure Compare the roles in the sample and check access rights to the environments.

Evidence Role matrix, authorisation extract of the environments

Step 06

BSI OPS.1.1.3

Tests and a documented acceptance take place before go-live.

Procedure For the sample, review the test plan, results and acceptance.

Evidence Test records, acceptance notes

Audit steps 7 to 9

Step 07 — BSI OPS.1.1.3

A rollback plan exists and is tested, or at least reviewed, for critical changes.

Procedure Read the rollback plans of the sample and, for failed changes, check whether they were applied.

Evidence Rollback plans, records of failed changes

Step 08 — BSI OPS.1.1.3

Emergency changes follow defined criteria and are approved and documented retrospectively within a deadline.

Procedure Select all emergency changes of the last half year and check justification, retrospective approval and documentation.

Evidence List of emergency changes, retrospective approvals

Step 09 — ISO/IEC 27001:2022 Annex A 8.9

After a change, configuration and system documentation are updated.

Procedure In the sample, check whether the configuration management contains the changed data.

Evidence Extract of configuration management before and after the change

Audit steps 10 to 13

Step 10 — ISO/IEC 27001:2022 Annex A 8.32

All actual changes go through the procedure; unrecorded changes are detected.

Procedure Compare system logs, deployments and configuration changes for a period with the change requests.

Evidence System logs, deployment logs, reconciliation list

Step 11 — BSI OPS.1.1.3

Affected parties are informed in time and maintenance windows are agreed.

Procedure Check the communication on the changes in the sample.

Evidence Announcements, maintenance calendar

Step 12 — ISO/IEC 27001:2022 Annex A 8.2

Access to make changes in production is limited to authorised people and is logged.

Procedure Extract the people authorised to change production, compare them with the roles and check logging.

Evidence Authorisation extract, log configuration

Step 13 — ISO/IEC 27001:2022 Annex A 8.32

Completed changes are reviewed afterwards and metrics on success rate and emergency changes are evaluated.

Procedure Review the post-implementation reviews of failed changes and the metric reports of the last twelve months.

Evidence Post-implementation reviews, metric reports, action list

Document request list

Request these 8 documents before you start

1. Process description for change management with catalogue of standard changes
2. List of all changes of the last six to twelve months with category and status
3. Change requests, approvals and test records of the sample
4. List of emergency changes with retrospective approval
5. Role matrix and authorisation extract for the productive environments
6. System logs and deployment logs for the reconciliation
7. Minutes of the change board
8. Metric reports on changes

TYPICAL FINDINGS

- Changes are requested after implementation; approval is dated after the change.
- Requests contain no rollback plan; for failed changes there is no evidence of recovery.
- Administrators change systems directly without a ticket; the reconciliation with system logs shows gaps.
- Requester and approver are the same person.
- Emergency changes make up a high share and are not approved retrospectively.
- Configuration management is not updated after changes.

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