Sample audit programme

Physical security of data centre

12 audit steps · ISO 27001, BSI

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

ISO/IEC 27001:2022 Annex A 7.1 · BSI INF.2 · ISO/IEC 27001:2022 Annex A 7.2 · ISO/IEC 27001:2022 Annex A 7.4 · ISO/IEC 27001:2022 Annex A 7.5 · ISO/IEC 27001:2022 Annex A 7.11 · ISO/IEC 27001:2022 Annex A 7.12 · BSI INF.12 · ISO/IEC 27001:2022 Annex A 7.13 · BSI INF.5 · ISO/IEC 27001:2022 Annex A 7.14 · ISO/IEC 27001:2022 Annex A 8.14

Audit objective and scope

The audit assesses whether the organisation divides its rooms for IT equipment into security zones, controls and monitors access effectively and protects equipment against environmental threats and loss of supply. It also assesses whether maintenance, inspections and emergency measures for building services are carried out demonstrably.

SCOPE

- Own data centres, server rooms and technical rooms, including distribution rooms at sites
- Access control, surveillance, fire protection, climate control, power supply and cabling
- Maintenance contracts and inspection records for building services
- Out of scope: provider data centres, which are considered separately through certificates or reports

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 7.1; BSI INF.2

Security zones are defined; rooms for IT equipment lie within a protected area with clear boundaries.

Procedure Review the zone plan and check boundaries, doors, windows and entrances during a walkthrough.

Evidence Zone plan, walkthrough record with photos

Step 02 — ISO/IEC 27001:2022 Annex A 7.2

Only authorised persons gain access; access rights are requested, approved and reviewed regularly.

Procedure Reconcile the list of persons with access against staff and provider lists and review the last recertification.

Evidence Access rights extract, approvals, review record

Step 03 — ISO/IEC 27001:2022 Annex A 7.2

Visitors and service providers are registered, escorted and their presence logged.

Procedure Reconcile the visitor book or electronic log of the last three months with maintenance visits.

Evidence Visitor log, maintenance records

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 7.4

Entrances and rooms are monitored; intrusion and door alarms are followed up.

Procedure Have the surveillance technology demonstrated and trace response and closure for three alarms.

Evidence Alarm logs, connection to control centre or security service

Step 05 — ISO/IEC 27001:2022 Annex A 7.5; BSI INF.2

Fire detection and suppression are in place, suited to the equipment and inspected; water hazards are considered.

Procedure Review the fire protection concept and inspection reports and check water pipes, detectors and suppression during the walkthrough.

Evidence Fire protection concept, inspection reports of fire detection and suppression systems

Step 06 — ISO/IEC 27001:2022 Annex A 7.11; BSI INF.2

Temperature and humidity are monitored; climate control is sized for the load and redundant.

Procedure Analyse readings for the last three months and check redundancy and alerting of the climate control.

Evidence Measurement logs, alerting concept, climate control sizing

Audit steps 7 to 9

Step 07

ISO/IEC 27001:2022 Annex A 7.11

Power supply is protected against failure; UPS and standby generator are tested under load regularly.

Procedure Review UPS and generator test records and compare bridging time with requirements.

Evidence Test records, capacity calculation, maintenance reports

Step 08

ISO/IEC 27001:2022 Annex A 7.12; BSI INF.12

Power and data cables are protected against damage and interception and are documented.

Procedure Inspect cable routes during the walkthrough and compare them with the documentation.

Evidence Cabling plan, walkthrough record

Step 09

ISO/IEC 27001:2022 Annex A 7.13

Equipment is maintained according to manufacturer requirements; maintenance work is traceable.

Procedure Reconcile the maintenance plan with maintenance records of the last twelve months for climate, UPS and fire protection.

Evidence Maintenance plan, maintenance reports, maintenance contracts

Audit steps 10 to 12

Step 10 — BSI INF.5

Decentralised technical rooms and distribution cabinets at sites are locked and protected against environmental threats.

Procedure Select two sites and check locking, access and surroundings of the technical rooms.

Evidence Site list, walkthrough records

Step 11 — ISO/IEC 27001:2022 Annex A 7.14

Equipment is handled before disposal or re-use so that no data falls into the wrong hands.

Procedure Trace the process for retired equipment from the data centre and request destruction evidence.

Evidence Disposal records, destruction evidence

Step 12 — ISO/IEC 27001:2022 Annex A 8.14

There is sufficient redundancy for the loss of a site, and site risks are assessed.

Procedure Review the site risk assessment and redundancy concept and assess distance and independence of the sites.

Evidence Site risk analysis, redundancy concept

Document request list

Request these 8 documents before you start

1. Zone plan and floor plans of rooms for IT equipment
2. Access rights extract and last review
3. Visitor logs
4. Fire protection concept and inspection reports
5. Temperature and humidity logs
6. UPS and standby generator test records
7. Maintenance plan and maintenance reports
8. Site risk analysis and redundancy concept

TYPICAL FINDINGS

- Access rights of former employees and providers are still active.
- Service providers work unescorted and unlogged in the server room.
- The standby generator has never been tested under load.
- Combustible materials are stored in the server room, water pipes run above the racks.
- Climate alarms go to an unattended mailbox.
- Technical rooms at sites are unlocked or used as storage.

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