Sample audit programme

Logging and monitoring

12 audit steps · ISO 27001, BSI, DORA

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

ISO/IEC 27001:2022 Annex A 8.15 · BSI OPS.1.1.5 · ISO/IEC 27001:2022 Annex A 8.17 · ISO/IEC 27001:2022 Annex A 8.16 · BSI DER.1 · DORA Art. 10(1) and (2) · DORA Art. 10(2) · DORA Art. 10(3) · DORA Art. 10(1) · BSI DER.2.1 · ISO/IEC 27001:2022 Annex A 8.15 and 5.22

Audit objective and scope

The audit assesses whether the organisation has defined which events are logged in which systems, whether logs are protected against alteration and whether effective monitoring detects anomalies and passes them into security incident handling. It also assesses whether time sources are aligned so that events remain traceable across systems.

SCOPE

- Servers, databases, directory services, network components, firewalls and applications used for essential services
- Central log collection, SIEM or comparable analysis, and alerting paths
- Operation by own staff and by service providers, where they generate or evaluate logs
- Out of scope: video surveillance and logging of customer applications, unless agreed separately

Audit steps 1 to 3

Step 01 — ISO/IEC 27001:2022 Annex A 8.15; BSI OPS.1.1.5

A policy defines which events are to be logged, how long logs are retained and who evaluates them.

Procedure Read the policy, establish approval and currency, and compare it with the system overview.

Evidence Logging policy with approval record, system overview

Step 02 — ISO/IEC 27001:2022 Annex A 8.15

For essential systems the events to be captured are defined, including log-ins, changes to rights, access to sensitive data and configuration changes.

Procedure Select five essential systems and compare the log sources actually enabled with the definition.

Evidence Logging concept per system, configuration extracts of logging

Step 03 — ISO/IEC 27001:2022 Annex A 8.15; BSI OPS.1.1.5

Logs are collected centrally, protected against alteration and deletion, and retained for the defined period.

Procedure Check access rights to the log store and retrieve sample logs from within the retention period.

Evidence Authorisation extract of the log store, retention settings, retrieval examples

Audit steps 4 to 6

Step 04 — ISO/IEC 27001:2022 Annex A 8.15

Administrators can neither change nor delete the logs of their own activity.

Procedure Check whether privileged accounts hold write or delete rights on logs and trace the separation of roles.

Evidence Role matrix, authorisation extract, log forwarding configuration

Step 05 — ISO/IEC 27001:2022 Annex A 8.17

System clocks are synchronised with agreed time sources so that events can be matched across systems.

Procedure Read time sources and deviations on a sample of servers and network components.

Evidence Time service configuration, extract of time deviation

Step 06 — ISO/IEC 27001:2022 Annex A 8.16; BSI DER.1; DORA Art. 10(1) and (2)

Monitoring detects anomalies in networks, systems and applications, with defined thresholds and rules for alerts.

Procedure Review the monitoring rule set, compare coverage of essential systems and ask about thresholds.

Evidence Monitoring rule catalogue, coverage overview, description of thresholds

Audit steps 7 to 9

Step 07

ISO/IEC 27001:2022 Annex A 8.16; DORA Art. 10(2)

Alerts reach the responsible people promptly, are assessed and are tracked until resolved.

Procedure Select ten alerts from the last six months and trace receipt, assessment, response time and closure.

Evidence Alert list, tickets, on-call schedule

Step 08

DORA Art. 10(3); BSI DER.1

Sufficiently qualified staff and hours are available for monitoring, including outside business hours.

Procedure Compare staffing, on-call model and cover arrangements with the alert volume.

Evidence Duty roster, on-call arrangement, statistics of alert volume

Step 09

DORA Art. 10(1); ISO/IEC 27001:2022 Annex A 8.16

Monitoring is tested for effectiveness at regular intervals, for example with simulated events, and gaps are closed.

Procedure Review test records of the last twelve months and check whether findings led to rule changes.

Evidence Test reports, rule changes, action list

Audit steps 10 to 12

Step 10 — BSI DER.1; BSI DER.2.1

Security-related events are passed into security incident handling and classified there.

Procedure For three alerts, check whether and how they were recorded and assessed as a security incident.

Evidence Incident register, link between alert and incident

Step 11 — ISO/IEC 27001:2022 Annex A 8.15 and 5.22

Logs from service providers and cloud services are available and included in the analysis.

Procedure For two outsourced services, check which logs are provided and whether they feed into monitoring.

Evidence Contract clauses on logs, connection of log sources

Step 12 — Good practice

Data protection for logs is regulated: access, purpose limitation and deletion periods for personal content are defined.

Procedure Review the rules on access and deletion and compare them with the works agreement or the data protection concept.

Evidence Data protection concept, deletion concept, agreement with the employee representation

Document request list

Request these 8 documents before you start

1. Logging and monitoring policy
2. System overview with logging concept per essential system
3. Configuration extracts of logging and time synchronisation
4. Monitoring rule catalogue and coverage overview
5. Alert list of the last six months with tickets
6. On-call schedule and escalation rules
7. Authorisation extract of the central log store
8. Test reports on monitoring

TYPICAL FINDINGS

- Essential systems produce no logs or only local logs that are not collected centrally.
- Administrators hold write or delete rights on the logs that record their activity.
- Time sources are not aligned, so events cannot be matched across systems.
- Alerts are generated but not assessed promptly; there is no on-call cover outside business hours.
- Monitoring has never been tested; rules date from the introduction and have not been adapted.
- Logs of service providers and cloud services are not connected.

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