Sample audit programme

# Security incidents and reporting

## 13 audit steps · NIS2, DORA, ISO 27001

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

ISO/IEC 27001:2022 Annex A 5.24 · BSI DER.2.1 · NIS2 Directive Art. 21(2)(b) · ISO/IEC 27001:2022 Annex A 6.8 · ISO/IEC 27001:2022 Annex A 5.25 · DORA Art. 18(1) · DORA Art. 17(2) · ISO/IEC 27001:2022 Annex A 5.26 · DORA Art. 17(3) · ISO/IEC 27001:2022 Annex A 5.28 · BSI DER.2.2 · NIS2 Directive Art. 23 · § 32(1) BSIG · DORA Art. 19(1) and (4) · GDPR Art. 33(1) and (5) · GDPR Art. 33(2) · ISO/IEC 27001:2022 Annex A 5.20 · NIS2 Directive Art. 20 · ISO/IEC 27001:2022 Annex A 5.27

## Audit objective and scope

The audit assesses whether the organisation runs an incident process covering reporting, assessment, classification, containment, recovery and review. It also assesses whether reporting duties towards authorities, supervisors and data subjects can be met within their deadlines, and whether responsibilities and deputies are clarified.

### SCOPE

- Security incidents in IT, applications, networks and at service providers that affect confidentiality, integrity or availability
- Reporting paths within the organisation and to authorities, supervisors, customers and data subjects
- Functions involved: information security, IT operations, data protection, legal, communications and management
- Out of scope: case-specific technical forensics and incident handling in physical security

## Audit steps 1 to 3

**Step 01** ISO/IEC 27001:2022 Annex A 5.24; BSI DER.2.1; NIS2 Directive Art. 21(2)(b)

### An incident handling process exists, is approved and defines roles, procedures and escalation.

**Procedure** Read the process description, check approval and currency and compare roles with the organisation.

**Evidence** Process description with approval, role overview, escalation plan

**Step 02** ISO/IEC 27001:2022 Annex A 6.8

### Employees and providers know the reporting path for events and can report anomalies at any time.

**Procedure** Check the reporting channel and how it is publicised, and ask two business units how reports are made.

**Evidence** Reporting path on the intranet, training material, interview notes

**Step 03** ISO/IEC 27001:2022 Annex A 5.25; DORA Art. 18(1)

### Events are assessed and classified as incidents against defined criteria; classification takes account of impact, duration and affected data or services.

**Procedure** Select ten events of the last twelve months and trace the classification against the criteria.

**Evidence** Classification scheme, event and incident register

## Audit steps 4 to 6

Step 04 — DORA Art. 17(2); ISO/IEC 27001:2022 Annex A 5.26

### All incidents are recorded in a register with cause, impact, measures and status.

**Procedure** Check the register for completeness of entries and compare it with reports from monitoring and the service desk.

**Evidence** Incident register, analysis of service desk and monitoring

Step 05 — ISO/IEC 27001:2022 Annex A 5.26; DORA Art. 17(3)

### Response plans are available for handling, describing containment, eradication and recovery and setting decision authority.

**Procedure** Read the response plans and check on two closed incidents whether they were applied.

**Evidence** Response plans, incident files, decision records

Step 06 — ISO/IEC 27001:2022 Annex A 5.28; BSI DER.2.2

### Evidence is preserved so that incidents remain traceable and legally usable later.

**Procedure** Check the evidence preservation procedure and its application in two incidents.

**Evidence** Procedure description, evidence of preservation, chain of custody record

## Audit steps 7 to 9

Step 07

NIS2 Directive Art. 23; § 32(1) BSIG

### The organisation can report significant security incidents within the deadlines: early warning within 24 hours, notification within 72 hours, final report after one month.

**Procedure** Trace the reporting process with responsibilities, templates and availability, and check a report or an exercise against the deadlines.

**Evidence** Reporting process, templates, authority contact list, evidence of exercise or report

Step 08

DORA Art. 19(1) and (4)

### For financial entities: major ICT-related incidents are reported to the competent authority in an initial notification, an intermediate report and a final report.

**Procedure** Check whether reporting paths, templates and responsibilities for the three reporting stages are defined and have been applied.

**Evidence** Reporting process, templates, evidence of reports

Step 09

GDPR Art. 33(1) and (5)

### Personal data breaches are assessed and, where required, reported to the supervisory authority within 72 hours; breaches are documented.

**Procedure** Check the assessment procedure, clarify cooperation with data protection and review documentation and reports of the last twelve months.

**Evidence** Data breach procedure, documentation of breaches, reports

## Audit steps 10 to 13

Step 10 — GDPR Art. 33(2); ISO/IEC 27001:2022 Annex A 5.20

### Service providers are obliged to report incidents without delay, and the reporting path is agreed.

**Procedure** Check the contracts of three providers for reporting deadlines and contact persons.

**Evidence** Contract clauses, contact lists

Step 11 — NIS2 Directive Art. 20; DORA Art. 17(3)

### Management and affected areas are informed of significant incidents, and external communication is regulated.

**Procedure** Trace escalation and reports to management in the sampled incidents and read the communication concept.

**Evidence** Escalation records, reports to management, communication concept

Step 12 — ISO/IEC 27001:2022 Annex A 5.27; DORA Art. 17(2)

### A review follows significant incidents, and its results feed into measures, training and adjustment of processes.

**Procedure** Review the post-incident reviews of the last twelve months and check implementation of the measures.

**Evidence** Review reports, action list, changes to plans

Step 13 — ISO/IEC 27001:2022 Annex A 5.24

### The incident process is exercised and the ability to report is tested regularly.

**Procedure** Review exercise records of the last twelve months and check whether the reporting path and deadlines were part of the exercise.

**Evidence** Exercise planning, exercise records, findings

Document request list

# Request these 8 documents before you start

1. Process description for security incident management
2. Classification scheme and response plans
3. Incident register of the last twelve months
4. Reporting process with templates, responsibilities and authority contact lists
5. Evidence of reports filed or exercises held
6. Documentation of personal data breaches
7. Contract clauses on incident reporting at service providers
8. Post-incident review reports

## TYPICAL FINDINGS

- Incidents are recorded in several systems, and a complete register is missing.
- There are no defined classification criteria; the assessment depends on the person acting.
- Responsibility and deputies for reports to authorities are not clarified, and deadlines would not be met.
- Data protection is involved late in incidents involving personal data.
- Service providers are not obliged to report quickly.
- Post-incident reviews do not take place or do not lead to tracked measures.

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