Sample audit programme

Business continuity management

14 audit steps · BSI 200-4, NIS2

14 audit steps with criterion, reference, procedure and expected evidence. 9 documents to request and the typical findings.

BSI standard 200-4 · BSI DER.4 · NIS2 Directive Art. 20 · ISO/IEC 27001:2022 Annex A 5.30 · NIS2 Directive Art. 21(2)(c) · NIS2 Directive Art. 23 · NIS2 Directive Art. 21(2)(d) · ISO/IEC 27001:2022 Annex A 5.29 · NIS2 Directive Art. 21(2)(f)

Audit objective and scope

The audit assesses whether a continuity management exists that knows the critical business processes and their dependencies, derives precautions and plans from them and shows through exercises that the plans hold in a real event. It also assesses whether management takes responsibility for the topic.

SCOPE

- Continuity management or BCM system with policy, roles, impact analysis, strategies and plans
- IT contingency planning and recovery for the critical processes
- Crisis communication, alerting and reporting channels
- Out of scope: fire protection and occupational safety in detail, unless agreed separately

Audit steps 1 to 3

Step 01 — BSI standard 200-4; BSI DER.4; NIS2 Directive Art. 20

A continuity management policy is approved by management and sets objectives, scope and responsibility.

Procedure Read the policy, check approval and currency, and trace the reporting line to management.

Evidence Policy with approval, management decisions

Step 02 — BSI standard 200-4; BSI DER.4

Roles for continuity management are filled, including continuity officers and crisis team, with deputies.

Procedure Check role descriptions, staffing and deputies, and test a sample of contact details for reachability.

Evidence Role descriptions, staffing list, contact list

Step 03 — BSI standard 200-4; BSI DER.4

An impact analysis has identified the critical processes, their recovery times and their dependencies.

Procedure Read method and results and confirm processes and dependencies with the business units on a sample basis.

Evidence Impact analysis, process list with recovery times, dependency overview

Audit steps 4 to 6

Step 04 BSI standard 200-4

Disruption scenarios and their likelihood are assessed and the results feed into planning.

Procedure Review the risk analysis for disruptions and check whether scenarios such as loss of a site, provider, IT or staff are included.

Evidence Risk analysis, scenario list

Step 05 BSI standard 200-4

Continuity and recovery strategies with the necessary resources are derived from the analysis and approved.

Procedure Compare strategies and resource planning with the results of the impact analysis.

Evidence Strategy documents, budget and resource planning

Step 06 BSI DER.4

Contingency and recovery plans exist for the critical processes and are available in a real event even without the main environment.

Procedure Read the plans for two critical processes and establish where they are stored and whether they are accessible offline.

Evidence Contingency plans, storage concept, evidence of access

Audit steps 7 to 10

Step 07 — ISO/IEC 27001:2022 Annex A 5.30; NIS2 Directive Art. 21(2)(c)

Recovery times and tolerable data loss of IT match the requirements of the processes.

Procedure Compare the process targets with the technical capabilities of IT and the results of recovery tests.

Evidence Comparison of targets, IT test records

Step 08 — BSI DER.4; NIS2 Directive Art. 23

Alerting, internal and external communication and the reporting channels for significant security incidents are defined.

Procedure Read the communication plan and trace the reporting channel through an example, including deadlines.

Evidence Communication plan, alerting list, reporting templates

Step 09 — NIS2 Directive Art. 21(2)(d)

Dependencies on service providers are recorded and secured by commitments for an emergency.

Procedure Select critical providers from the impact analysis and check contractual commitments on availability and support in an emergency.

Evidence Provider list, contracts, provider confirmations

Step 10 — BSI standard 200-4; BSI DER.4; ISO/IEC 27001:2022 Annex A 5.30

Exercises and tests are planned, carried out and evaluated, and the results lead to improvements.

Procedure Check the exercise plan and reports of the last two years and establish which actions followed from the results.

Evidence Exercise plan, exercise reports, action list

Audit steps 11 to 14

Step 11 — BSI DER.4

Participants are trained and made aware of their tasks in an emergency.

Procedure Check the training plan and attendance lists and ask a sample of participants about their tasks.

Evidence Training plan, attendance lists

Step 12 — ISO/IEC 27001:2022 Annex A 5.29

During a disruption, security measures such as access controls remain effective in emergency operation.

Procedure Check emergency operating procedures for planned exceptions to access and protection measures and their approval.

Evidence Emergency operating procedures, exception approvals

Step 13 — BSI standard 200-4

Plans are updated after changes and incidents and maintained with a version history.

Procedure Compare the change history of the plans with organisational changes and incidents of the last year.

Evidence Version history, incident reports, change requests

Step 14 — BSI standard 200-4; NIS2 Directive Art. 21(2)(f)

Management reviews the continuity management regularly and decides on improvements.

Procedure Review management reviews and reports of the last two years and follow up decisions.

Evidence Management review, reports, decisions

Document request list

Request these 9 documents before you start

1. Continuity management policy
2. Role descriptions, staffing and contact list
3. Impact analysis with process list and recovery times
4. Risk analysis and scenario list
5. Contingency and recovery plans for the critical processes
6. Communication and alerting plan
7. Exercise plan and exercise reports of the last two years
8. Contracts and commitments of critical providers
9. Management review of continuity management

TYPICAL FINDINGS

- The impact analysis is outdated or does not cover essential processes.
- Plans are stored only on systems that would fail in a real event.
- Exercises are limited to tabletop games; a technical recovery has never been tested.
- Recovery times of the processes and the capabilities of IT do not match.
- Roles are not filled or contact details are out of date.
- Plans were not adjusted after organisational 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