Sample audit programme

Cryptography and key management

12 audit steps · NIS2, BSI, ISO 27001

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

NIS2 Directive Art. 21(2)(h) · § 30(2) no. 8 BSIG · BSI CON.1 · BSI TR-02102-1 · ISO/IEC 27001:2022 Annex A 8.24 · BSI TR-02102-2 · DORA Art. 9(4)(d) · ISO/IEC 27001:2022 Annex A 5.3 · ISO/IEC 27001:2022 Annex A 8.13 · ISO/IEC 27001:2022 Annex A 5.31

Audit objective and scope

The audit assesses whether the organisation governs the use of cryptography in a cryptographic concept, uses only recognised algorithms and key lengths and encrypts data in transit and at rest according to its protection needs. It also assesses whether keys and certificates are managed in a controlled way from generation to destruction and whether the organisation is prepared for future changes of algorithms.

SCOPE

- Encryption of data in transit and at rest in applications, databases, storage media and backups
- Key management including hardware security modules, key vaults and cloud key services
- Internal and external certificates and an own public key infrastructure, where present
- Out of scope: cryptanalysis of individual algorithms

Audit steps 1 to 3

Step 01 — NIS2 Directive Art. 21(2)(h); § 30(2) no. 8 BSIG; BSI CON.1

A cryptographic concept defines where and how cryptography is used and is approved.

Procedure Read the concept, check approval and currency and compare it with the systems in use.

Evidence Cryptographic concept with approval note

Step 02 — BSI TR-02102-1

Permitted algorithms and key lengths follow recognised recommendations; outdated algorithms are excluded.

Procedure Compare the list of permitted algorithms with current recommendations and read actual settings on three systems.

Evidence List of permitted algorithms, configuration extracts

Step 03 — BSI CON.1; ISO/IEC 27001:2022 Annex A 8.24

A register of cryptographic algorithms, keys and certificates in use is maintained.

Procedure Review the register and check completeness against a sample of applications and interfaces.

Evidence Crypto inventory, certificate list

Audit steps 4 to 6

Step 04 — BSI TR-02102-2; ISO/IEC 27001:2022 Annex A 8.24

Data is encrypted in transit over networks; the TLS configuration meets the requirements.

Procedure Test external and internal services with a tool for protocol versions and cipher suites.

Evidence TLS configuration test results, actions on deviations

Step 05 — ISO/IEC 27001:2022 Annex A 8.24; DORA Art. 9(4)(d)

Stored data is encrypted according to protection needs and risk assessment, including backups.

Procedure For three data sets with high protection needs, trace encryption of database, storage and backup.

Evidence Protection needs assessment, encryption configuration

Step 06 — ISO/IEC 27001:2022 Annex A 8.24; BSI CON.1

The key life cycle is governed: generation, distribution, storage, rotation, revocation and destruction.

Procedure Read the rule and trace the life cycle of two keys including the date of the last rotation.

Evidence Key management rule, key rotation records

Audit steps 7 to 9

Step 07 — DORA Art. 9(4)(d); ISO/IEC 27001:2022 Annex A 8.24

Keys are stored in protected form, for example in hardware security modules or key vaults, with tightly limited access.

Procedure Ask where keys are stored, have a search run for keys in source code or configuration files and check access rights.

Evidence Key vault permission extract, result of the search for embedded keys

Step 08 — ISO/IEC 27001:2022 Annex A 8.24

Certificates are monitored centrally, renewed in time and revoked when compromised.

Procedure Have expiry monitoring demonstrated and ask about outages caused by expired certificates in the last twelve months.

Evidence Certificate overview with expiry dates, renewal records, incident list

Step 09 — ISO/IEC 27001:2022 Annex A 5.3

Duties in key management are segregated; critical operations require dual control.

Procedure Check roles in key management and records of critical operations such as generating master keys.

Evidence Role concept, records with two participants

Audit steps 10 to 12

Step 10 — BSI CON.1; ISO/IEC 27001:2022 Annex A 8.13

Keys are backed up so that encrypted data and backups can be restored.

Procedure Have key backup explained and review the last restore test of encrypted data.

Evidence Key backup concept, restore test record

Step 11 — ISO/IEC 27001:2022 Annex A 5.31

Legal requirements on the use and export of cryptography are taken into account.

Procedure Check whether legal restrictions have been identified for sites and travel outside the EU.

Evidence Register of legal requirements, rule for sites abroad

Step 12 — BSI TR-02102-1

The organisation plans the transition to new algorithms, including quantum-resistant cryptography.

Procedure Ask whether systems with long-lived data and hard-coded algorithms are recorded and whether a transition plan exists.

Evidence Crypto agility analysis, migration plan

Document request list

Request these 8 documents before you start

1. Cryptographic concept
2. List of permitted algorithms and key lengths
3. Crypto inventory and certificate overview
4. TLS configuration test results
5. Key management rule with roles
6. Permission extract of key vaults or hardware security modules
7. Record of the last restore test of encrypted data
8. Plan for the transition of cryptographic algorithms

TYPICAL FINDINGS

- A cryptographic concept is missing or lists algorithms that are no longer recommended.
- Keys and passwords are kept in source code or configuration files.
- Certificates expire unnoticed and cause outages.
- Internal services accept outdated protocol versions.
- Backups are encrypted, but the key is not backed up separately.
- There is no overview of which systems would be affected by a change of algorithms.

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