NIS2

NIS2 (whole Part)

Audit Checklist

46 audit questions across **6** sections.

HOW TO USE THIS CHECKLIST

Each question has three boxes the auditor fills in during the audit:

1. **Compliance** — the binary headline: Compliant / Non-compliant.
2. **Classification** — where the gap is, four-state grid: Documented / Implemented matrix.
3. **Finding level** — severity: Maj / Min / Obs (Major nonconformity / Minor nonconformity / Observation).

Severity is the auditor's call on the day, against the real finding — no severity is pre-suggested per question.

auditchecklists.org Audit Checklist Licence

Product:	NIS2 (whole Part) (46 questions)
Regulation:	
Issued:	[YYYY-MM-DD — STAMPED AT ISSUE]

Licensed to:	[ORG NAME — STAMPED AT ISSUE]
Licensee email:	[EMAIL — STAMPED AT ISSUE]
Order:	[AVI-YYYY-NNNNN — STAMPED AT ISSUE]

Licence terms

This audit checklist is licensed for use within the organisation named above by the licensee email named above. Use is permitted by employees and contractors of the named organisation in the course of their work for that organisation, including printing, internal distribution within the organisation, annotation during audits, and incorporation into the organisation's management-system documentation as a working reference.

Not for redistribution. Sharing this document, or any derivative or extract of it, with any party outside the named organisation is a breach of this licence. This includes posting to file-sharing networks, internal wikis or knowledge bases accessible to other organisations, vendor portals, supplier-facing GRC systems, and email forwarding to colleagues at other firms. Quoting individual audit questions in regulator submissions or internal training materials is permitted; reproducing the structured checklist as a whole is not.

Each additional organisation or operating site requires a separate licence. If a sister organisation in the same group, or a separate operating entity, requires the same checklist, contact licences@auditchecklists.org for a multi-site licence quote. Holding companies licensing for multiple subsidiaries are eligible for group-licence pricing.

Licence transfers. This licence does not transfer with sale, merger, or organisational restructure without written consent. auditchecklists.org may, at its discretion, transfer the licence to the successor organisation on request — usually a formality, contact licences@auditchecklists.org.

Defects and amendments. If you identify a defect in this checklist — wrong content, mistranscribed regulation, factual error — email support@auditchecklists.org. We will verify the defect, correct it, and reissue the affected artefacts to you within a reasonable timeframe at no further charge. Regulatory amendments published during your 12-month update

§Article 20

Governance

Q1 ARTICLE NIS2

Has the management body formally approved the Art. 21 cybersecurity risk-management measures — by a documented decision identifying what was approved, when, and on the basis of what evidence?

SOURCE VERBATIM

> 1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.
>
> — Directive (EU) 2022/2555 Article 20(1) — management body approves measures, Original 2022-12-14 (NIS2)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Management body minute(s) approving the cybersecurity risk-management measures
- The measure set put before the body — risk register, control inventory, gap analysis
- Periodic re-approval cycle on material changes (new acquisitions, major incidents, technology shifts)
- Briefing pack provided to the body before the approval decision
- For matrix or group structures: which body holds the approval right per entity

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q2 ARTICLE NIS2

Does the management body actively oversee the implementation of the approved cybersecurity measures — receiving regular reports on coverage, incidents, audit findings, and corrective actions, and acting on them?

SOURCE VERBATIM

> 1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.
>
> — Directive (EU) 2022/2555 Article 20(1) — management body oversees implementation, Original 2022-12-14 (NIS2)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Oversight cadence — frequency and content of body-level reports
- Sample of recent reports the body has received
- Decision records where the body acted on a report (resource allocation, accepted residual risk, ordered remediation)
- Tracking of corrective actions raised under §21(4) up to the body
- KPI / KRI dashboard the body uses

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES:

Q3 ARTICLE NIS2

Do members of the management body actually follow cybersecurity training — sufficient for them to identify risks and assess the entity's cybersecurity risk-management practices and the impact on services?

SOURCE VERBATIM

> 1. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.
>
> — Directive (EU) 2022/2555 Article 20(2) — management body training, Original 2022-12-14 (NIS2)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Training programme for management-body members — content, depth, format
- Completion records per body member, including new appointments
- Refresh cycle and triggers (incidents, technology change, regulatory updates)
- Effectiveness check — pre/post assessment, decision-quality review
- For board / non-executive directors: tailored content reflecting their oversight role rather than operator-level detail

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES: