NIS2 implementing acts (Reg 2024/2690) (whole Part)

Audit Checklist

328 audit questions across **26** 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 implementing acts (Reg 2024/2690) (whole Part) (328 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

§Annex §1

Policy on the security of network and information systems (NIS2 Art. 21(2)(a))

Q1 ANNEX NIS2-IMPL Annex.1.1.1(a)

Does the NIS policy set out the entity's approach to managing the security of its network and information systems — articulated specifically enough that a reader can describe how the entity manages risk?

SOURCE VERBATIM

> 1.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the policy on the security of network and information systems shall:
>
> (a) set out the relevant entities' approach to managing the security of their network and information systems;
>
> — Commission Implementing Regulation (EU) 2024/2690 Annex §1.1.1(a), Original 2024-10-17 (NIS2-IMPL)

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

- Current NIS policy
- Section articulating the approach
- Cross-reference to risk-management methodology (Annex §2)

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q2 ANNEX NIS2-IMPL Annex.1.1.1(b)

Is the NIS policy appropriate to — and complementary with — the entity's business strategy and objectives, so security is aligned with the business rather than running in parallel to it?

SOURCE VERBATIM

> (b) be appropriate to and complementary with the relevant entities' business strategy and objectives;
> — Commission Implementing Regulation (EU) 2024/2690 Annex §1.1.1(b), Original 2024-10-17 (NIS2-IMPL)

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

- Business-strategy alignment statement in policy
- Linkage between security objectives and business objectives
- Sign-off by senior leadership on alignment

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q3 ANNEX NIS2-IMPL Annex.1.1.1(c)

Does the NIS policy explicitly set out the network and information security objectives the entity is pursuing?

SOURCE VERBATIM

> (c) set out network and information security objectives;
> — Commission Implementing Regulation (EU) 2024/2690 Annex §1.1.1(c), Original 2024-10-17 (NIS2-IMPL)

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

- Objectives section in the policy
- Measurability — KPIs/KRIs linked to objectives

MANAGEMENT SYSTEM REFERENCE:

_____

FINDINGS / NOTES: