

NIS2

Readiness checklist

A practical overview of key areas for essential and important entities.

ORGANISATION	REVIEW DATE	RESPONSIBLE PERSON

How to use: tick implemented measures; add outstanding items to an action plan.

01 Identifying your obligations

Arts. 2, 3, 4, 5 and 26

- ☐ We assessed our sector, entity type, size and exceptions under Annexes I and II.
- ☐ We documented whether we are an essential or important entity.
- ☐ We identified the applicable national law, jurisdiction and competent authority.
- ☐ We checked registration duties, local deadlines and any sector-specific EU rules.

02 Management accountability

Art. 20; Art. 21(2)(g)

- ☐ Management approved cybersecurity measures and oversees implementation.
- ☐ Risk, control and incident-reporting responsibilities have named owners.
- ☐ Management receives training; staff receive cyber hygiene and security training.

03 Risk management and continuity

Art. 21(1); Art. 21(2)(a)-(c), (i)

- ☐ We maintain security policies and an inventory of assets and critical services.
- ☐ Our risk assessment covers systems, physical risks and service dependencies.
- ☐ Measures are proportionate to risk, exposure and the potential impact of incidents.
- ☐ Incident response, business continuity and crisis-management plans are in place.
- ☐ Backups, recovery arrangements and response roles are tested in practice.

What does a ticked item mean?

A measure is documented, implemented, maintained and evidenced in practice. Use this checklist alongside the national law that applies to your organisation.

Implementation and follow-up

The remaining checklist items and the next practical steps.

04 Security measures in practice

Art. 21(2)(e), (h)-(j)

- ☐ We manage personnel security, identities, access rights and privileged accounts.
- ☐ Acquisition, development and maintenance include security requirements.
- ☐ We handle vulnerabilities and define how they are disclosed.
- ☐ Policies cover cryptography and, where appropriate, encryption.
- ☐ We use appropriate MFA or continuous authentication and secure communications.

05 Supply chain security

Art. 21(2)(d); Art. 21(3)

- ☐ We assess security risks involving direct suppliers and service providers.
- ☐ Supplier requirements reflect their vulnerabilities and cybersecurity practices.

06 Incident reporting

Art. 23

- ☐ We defined significant-incident criteria and internal escalation responsibilities.
- ☐ We know the reporting channel, CSIRT or authority and applicable deadlines.
- ☐ Procedures cover warnings, notifications, requested updates and final reports.

07 Effectiveness and evidence

Art. 21(2)(f); Art. 21(4)

- ☐ We assess control effectiveness and keep evidence of implementation and tests.
- ☐ Gaps have owners, due dates and tracked corrective actions.

SIGNIFICANT INCIDENT: REPORT WITHOUT UNDUE DELAY

24 h

Early warning

72 h

Incident notification

1 month

Final report

24 h and 72 h run from awareness of a significant incident; the final report is due within one month of notification. Trust service providers must notify significant incidents affecting trust services within 24 h. If ongoing, submit a progress report, then a final report within one month of handling the incident.

NEXT ACTION

OWNER / DUE DATE

[NIS2: official text](#)

[Regulation \(EU\) 2024/2690](#)

[ENISA guidance](#)

Informational aid, not legal advice or proof of compliance. National rules may add duties. Regulation 2024/2690 applies to specified digital entities; check whether it covers you.