NIS2 Compliance Checklist — Article 21(2)

All ten risk management measures with the ISMS gap assessment — v1.0 · 2026-07-16

#	Measure (Art. 21(2))	ISMS coverage	The gap	What to do	Priority
(a)	**Risk analysis and information system security policies**	Covered by ISMS	—	Ensure the risk analysis covers the NIS2-specific operational aspects: incident reporting, supply chain, proof of effectiveness.	**Low**
(b)	**Incident handling**	Foundation — add operational layer	Operational 24h/72h capability under time pressure — coordination across security, legal, communications and management.	Build incident management beyond the plan: tabletop exercises against the 24-hour deadline; templates for all three reporting stages.	**High**
(c)	**Business continuity and crisis management**	Covered by ISMS	—	Verify BCM plans cover cyber incidents with simultaneous Article 23 reporting obligations.	**Low**
(d)	**Supply chain security**	Foundation — add operational layer	Continuous monitoring instead of annual snapshots; event-triggered re-assessments; retrievable supplier evidence.	Build monitoring capability; shift from cyclical to trigger-based assessments; add NIS2 clauses to contracts; make evidence retrievable on demand.	**High**
(e)	**Security in acquisition, development and maintenance**	Covered by ISMS	Check vulnerability disclosure against ENISA implementation guidance.	Verify that vulnerability disclosure processes meet the NIS2/ENISA expectations, which go beyond typical ISMS implementations.	**Medium**
(f)	**Effectiveness assessment of risk-management measures**	Foundation — add operational layer	Continuous evidence availability, not audit-cycle documentation.	Shift evidence management to continuous availability: versioning, validity periods, ownership; be able to answer authority requests within days.	**High**
(g)	**Cyber hygiene and cybersecurity training**	Covered by ISMS	Demonstrable executive training participation.	Ensure the management body demonstrably participates in cybersecurity training — this evidence is directly liability-relevant.	**Low**
(h)	**Cryptography and encryption**	Covered by ISMS	—	Keep cryptography policies current and aligned with the state of the art.	**Low**
(i)	**Personnel security, access control and asset management**	Covered by ISMS	—	Confirm MFA coverage where NIS2 requires it (see measure (j)).	**Low**
(j)	**MFA, secured communications and emergency communications**	Partially covered	Secured emergency communication channels that work independently of the regular (possibly compromised) infrastructure.	Audit MFA coverage; establish emergency channels independent of regular infrastructure; ensure encrypted communication for incident coordination.	**Medium**

Art 23 & Art 20 Duties

Obligation	Deadline / rule	Legal basis
Early warning to the CSIRT or competent authority	Within 24 hours of becoming aware of a significant incident	Art. 23(4)(a)

Obligation	Deadline / rule	Legal basis
Incident notification	Within 72 hours of becoming aware — assessment incl. severity, impact, indicators of compromise	Art. 23(4)(b)
Final report	Within one month of the incident notification	Art. 23(4)(d)
Management approval and oversight of risk-management measures	Ongoing — the management body approves the measures, oversees implementation and can be held liable	Art. 20(1)
Cybersecurity training for the management body	Regular — members of the management body are required to follow training	Art. 20(2)

How to use this checklist

1. Walk through each of the ten Article 21(2) measures and assess honestly: not 'do we have a process?' but 'can we operationally execute this under time pressure, against external parties, with verifiable evidence?'

2. Use the priority column as the starting point: the three High gaps (incident handling, supply chain, proof of effectiveness) carry the highest regulatory urgency.

3. For each gap, plan the operational build: which system, process or capability is concretely needed.

4. Keep the ISMS as the internal control layer and supplement it with the operational layer NIS2 additionally requires.

5. Track status, owner and evidence per measure in the checklist sheet — supervisory authorities can request evidence at any time.

Full explanations per measure, sources and the ISMS gap analysis:
https://www.orbiqhq.com/eu-regulations/nis2-compliance-checklist-article-21