NIS2 gap analysis template — Article 21(2) & Article 23

Ansvar AI · ansvar.eu/templates/nis2-gap-analysis · free to use, no email gate · generated 2026-07-02

This is the print companion to the XLSX workbook. The workbook has three sheets: a **gap register** with one row per NIS2 Art. 21(2) risk-management measure (a)–(j), an **incident-reporting tracker** for the Art. 23 obligations, and an **About** sheet with source and license. Requirement wording follows Directive (EU) 2022/2555 as published on EUR-Lex.

Working version with verdict dropdowns (Compliant / Partial / Gap): **ansvar.eu/templates/ansvar-nis2-gap-analysis-template.xlsx**

Sheet 1 — Gap register (Art. 21(2)(a)–(j))

Ref	Requirement (NIS2 Art. 21(2))	Current state	Verdict	Remediation	Owner	Due
21(2)(a)	Policies on risk analysis and information system security.	—	—	—	—	—
21(2)(b)	Incident handling.	—	—	—	—	—
21(2)(c)	Business continuity, such as backup management and disaster recovery, and crisis management.	—	—	—	—	—
21(2)(d)	Supply chain security, including security-related aspects of the relationships with direct suppliers and service providers.	—	—	—	—	—
21(2)(e)	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.	—	—	—	—	—
21(2)(f)	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	—	—	—	—	—
21(2)(g)	Basic cyber hygiene practices and cybersecurity training.	—	—	—	—	—
21(2)(h)	Policies and procedures on the use of cryptography and, where appropriate, encryption.	—	—	—	—	—
21(2)(i)	Human resources security, access control policies and asset management.	—	—	—	—	—
21(2)(j)	Multi-factor or continuous authentication, secured voice, video and text communications and secured emergency communication systems, where appropriate.	—	—	—	—	—

Sheet 2 — Incident reporting (Art. 23)

- **Significance test (23(3))** — severe operational disruption or financial loss; or considerable damage to others.
- **Early warning (23(4)(a))** — within 24 hours of becoming aware.
- **Incident notification (23(4)(b))** — within 72 hours, with an initial severity and impact assessment.
- **Intermediate report (23(4)(c))** — on request of the CSIRT or competent authority.
- **Final report (23(4)(d))** — not later than one month after the notification.
- **Recipient notification (23(1)–(2))** — notify affected service recipients; communicate remedies for significant cyber threats.

How to use it

- Fill the current-state column from your real policies, runbooks and contracts — not from intentions.
- Set a verdict per row: Compliant, Partial, or Gap. Evidence beats optimism.
- Give every Partial and Gap a remediation, an owner, and a due date.
- Test the Art. 23 sheet against a clock: could you file an early warning 24 hours from now?

Prefer it filled in and cited? A worked sample of the same register: **ansvar.eu/services/sample-gap-analysis**