REGUVARA · FREE PRACTICAL GUIDE

NIS2: Prepare reporting routes and evidence

A practical first step for management, IT/security, legal and compliance teams. Understand scope, the main reporting deadlines and five actions to start with.

Purpose: make the right questions visible quickly. This guide does not determine whether a specific legal entity is in scope of NIS2.

1. Make an initial scope assessment

- Map the entity's activity, service and legal entity to the sectors in Annexes I and II of the NIS2 Directive. A sector label alone does not settle scope.
- Check size, group links, service type, critical designations, exemptions and the relevant Member State's rules. Some entities or services may be covered regardless of the usual size threshold.
- For each potentially affected entity, record countries, sites, services, competent authority, registration and contact obligations, and the reasoning.

2. EU reporting stages for a significant incident

Stage	EU baseline under Article 23	Preparation prompt
Early warning	Without undue delay and no later than 24 hours after becoming aware of the significant incident.	Who starts the clock, decides, and identifies the right authority?
Incident notification	Without undue delay and no later than 72 hours after awareness; initial severity and impact assessment, with indicators where available.	How are facts, timestamps and unknowns collected in parallel?
Intermediate report	If requested by the CSIRT or competent authority.	Who tracks changes and answers follow-up questions?
Final report	Generally within one month of the incident notification. For an ongoing incident, a progress report is due then and the final report within one month after handling.	Who confirms the local deadline and required contents?

These deadlines concern significant incidents and awareness of them. Trust service providers have a special 24-hour incident-notification rule. Check national transposition, sector rules and other applicable EU laws.

WORKSHEET

From legal text to a first working process

NIS2 requires risk-based and proportionate technical, operational and organisational measures. Use this overview to bring the right owners together.

3. Topics addressed by Article 21

Measures protect the network and information systems used for services, including their physical environment. Scope and design depend on risk and proportionality.

Area	Example working question
Risk analysis and system security	Which services, systems, threats and dependencies are in scope? Who refreshes the assessment?
Incident handling	How are detection, classification, containment, escalation, evidence and lessons organised?
Continuity and crisis	Are backups, recovery, crisis roles and recovery objectives documented and tested?
Supply chain	Are direct suppliers, providers, critical dependencies and security information recorded?
Secure acquisition and development	How are systems selected and maintained securely, and vulnerabilities handled or disclosed?
Effectiveness review	How does the organisation determine whether security measures work?
Cyber hygiene and training	Which baseline practices and training are planned and evidenced?
Cryptography	What rules apply to cryptography and, where appropriate, encryption?
People, access and assets	How are permissions, staff changes, assets and access controlled?
Authentication and communication	Where are MFA or continuous authentication, secure communications and emergency channels appropriate?

4. Five useful first steps

- Appoint an owner to coordinate scope questions and open issues.
- Inventory services, legal entities, systems and critical direct suppliers.
- Name management, incident lead, IT/security, legal/compliance and communications roles, with deputies.
- Verify the national competent authority, CSIRT, registration, reporting channel and any sector duties.
- Run a short exercise: detect an incident, capture awareness time, escalate and build a fact record.

NIS2 does not automatically apply to every company. Scope depends on activity, size, legal entity, Member State, special cases and sector rules.

SOURCES AND LEGAL STATUS

Primary source: Directive (EU) 2022/2555, especially Articles 2-4, 20, 21 and 23 and Annexes I-II. Proposal COM(2026) 13 final is not law. On 8 October 2026, European Parliament procedure 2026/0012(COD) was awaiting a committee decision; a draft committee report had been published on 24 September 2026. National transposition and sector rules have not been reviewed country by country.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal