



FREE RESOURCE · SELF-ASSESSMENT

NIS2 Compliance Checklist

47 checks to diagnose your NIS2 readiness in about ten minutes. Each one points to the article it comes from, so you can check the source yourself.

Angel Sulev · Chief Architect of Secure AI · ANSULEV Group

Legal status checked: **2026-10-07** · Version 1.0

ansulev.com · info@ansulev.com

How to use this checklist

Answer each item honestly: **Yes** (in place and evidenced), **Partial** (exists but undocumented, untested or incomplete) or **No**. If you cannot show the evidence, the answer is Partial.

- References point to Directive (EU) 2022/2555 (NIS2) unless marked otherwise.
- Items tagged **ES** come from Spain's draft transposition law and may change before it is enacted.
- Score yourself at the end. The bands are a prioritisation aid, not a legal opinion.

What is at stake

- Fines for breaching Art. 21 or 23: at least up to **€10M or 2%** of worldwide turnover for essential entities, **€7M or 1.4%** for important entities, whichever is higher (Art. 34(4)–(5)).
- Management bodies approve the measures, oversee them and **can be held liable** (Art. 20(1)). In essential entities, a CEO or legal representative can be temporarily barred from managerial functions (Art. 32(5)(b)).
- Incident clock: **24h** early warning, **72h** notification, **one month** final report (Art. 23(4)).

Spain: where things stand on 2026-10-07

- NIS2 is **not yet transposed** in Spain. The *Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad* was approved by the Council of Ministers on 14 January 2025 and has not been published in the BOE.
- On 8 July 2026 the European Commission referred Spain, France, Ireland and the Netherlands to the Court of Justice for failing to notify full transposition.
- Until the new law is in force, **RD-ley 12/2018** and **RD 43/2021** (NIS1) still apply. Reference CSIRTs: INCIBE-CERT (private sector) and CCN-CERT (public sector).
- The draft mirrors the 24h / 72h / one-month timeline, creates a *Centro Nacional de Ciberseguridad*, and uses the ENS (RD 311/2022) as the baseline for security measures.

The EU obligations are already fixed, and building an evidenced programme takes months, so waiting for the BOE costs you that time.

1 • Scope and registration

#	CHECK	REFERENCE	STATUS
01	You have mapped every service you provide against the sectors and subsectors in Annex I (high criticality) and Annex II (other critical sectors).	Art. 2(1), Annex I–II	☐ Y ☐ P ☐ N
02	You have checked whether your organisation is medium-sized or larger : 50+ staff, or annual turnover and balance sheet both above €10M, counting partner and linked enterprises.	Art. 2(1); Rec. 2003/361/EC	☐ Y ☐ P ☐ N
03	You have checked the size-independent triggers : telecoms, trust services, TLD/DNS, domain registration, sole national provider of an essential service, critical entity, public administration.	Art. 2(2)–(4)	☐ Y ☐ P ☐ N
04	You know whether you are an essential or an important entity, and the reasoning is written down.	Art. 3(1)–(2)	☐ Y ☐ P ☐ N
05	You have identified sector-specific EU law with equivalent requirements that may take precedence (for example DORA for financial entities).	Art. 4	☐ Y ☐ P ☐ N
06	Registration data is ready: name, address, contact details including email, phone and IP ranges , sector, Member States served. Changes are reported within two weeks.	Art. 3(4); Art. 27 (digital providers)	☐ Y ☐ P ☐ N
07	A Responsable de la Seguridad de la Información (person, unit or committee, with a named substitute) is designated as contact point with the authority and CSIRT. ES	ES draft Art. 16	☐ Y ☐ P ☐ N
08	You know whether the ENS (RD 311/2022) applies to you. In the draft, the ENS NIS2 compliance profile accredits the measures, essential entities must certify, and important entities may self-assess. ES	ES draft Art. 15(2), 15(4)	☐ Y ☐ P ☐ N

2 • Governance and management accountability

#	CHECK	REFERENCE	STATUS
09	The management body has formally approved the cybersecurity risk-management measures, with a dated record.	Art. 20(1)	☐ Y ☐ P ☐ N
10	The management body oversees implementation through recurring reporting on status, gaps and incidents.	Art. 20(1)	☐ Y ☐ P ☐ N
11	Members of the management body have completed cybersecurity training , and attendance is recorded.	Art. 20(2)	☐ Y ☐ P ☐ N
12	Similar training is offered to employees on a regular basis .	Art. 20(2)	☐ Y ☐ P ☐ N
13	Directors understand their personal accountability , including liability for infringements and, in essential entities, possible temporary bans from managerial functions.	Art. 20(1), 32(5) (b), 32(6)	☐ Y ☐ P ☐ N
14	A named, adequately resourced owner of NIS2 compliance reports directly to the board.	Art. 20(1); ES draft Art. 16(4)	☐ Y ☐ P ☐ N

3 • Risk-management measures (Article 21)

The ten minimum measures of Art. 21(2), points (a) to (j), plus proportionality and supply-chain depth.

#	CHECK	REFERENCE	STATUS
15	A documented information-system security policy exists, is approved and is reviewed on a schedule.	Art. 21(2)(a)	☐ Y ☐ P ☐ N
16	A risk analysis is maintained using an all-hazards approach that includes the physical environment of your systems.	Art. 21(1)–(2)(a)	☐ Y ☐ P ☐ N
17	An incident handling procedure covers detection, triage, containment, recovery and lessons learned.	Art. 21(2)(b)	☐ Y ☐ P ☐ N
18	Logging and monitoring are good enough to detect an incident and reconstruct what happened.	Art. 21(2)(b)	☐ Y ☐ P ☐ N
19	Backups are defined, protected against tampering, and restores are tested .	Art. 21(2)(c)	☐ Y ☐ P ☐ N
20	A disaster recovery plan with recovery objectives exists and has been exercised.	Art. 21(2)(c)	☐ Y ☐ P ☐ N
21	Crisis management is defined: roles, decision rights and out-of-band communication.	Art. 21(2)(c)	☐ Y ☐ P ☐ N
22	You keep an inventory of direct suppliers and service providers, ranked by criticality.	Art. 21(2)(d)	☐ Y ☐ P ☐ N
23	Critical suppliers are assessed for their vulnerabilities, product quality and secure development practices.	Art. 21(3)	☐ Y ☐ P ☐ N
24	Supplier contracts include security requirements, incident notification duties and audit rights.	Art. 21(2)(d)	☐ Y ☐ P ☐ N
25	You take into account the EU coordinated risk assessments of critical supply chains (for example 5G).	Art. 21(3), 22(1)	☐ Y ☐ P ☐ N
26	Security is built into acquisition, development and maintenance : secure development and change management.	Art. 21(2)(e)	☐ Y ☐ P ☐ N
27	Vulnerability management runs continuously: scanning, prioritised patching, tracked deadlines.	Art. 21(2)(e)	☐ Y ☐ P ☐ N
28	A public vulnerability disclosure channel lets outsiders report flaws to you.	Art. 21(2)(e); Art. 12	☐ Y ☐ P ☐ N
29	The effectiveness of your measures is assessed on a schedule: audits, tests, metrics.	Art. 21(2)(f)	☐ Y ☐ P ☐ N
30	Any gap you find triggers corrective action without undue delay , and it is tracked to closure.	Art. 21(4)	☐ Y ☐ P ☐ N
31	A cyber hygiene baseline is enforced: hardening, secure configuration, patching, least functionality.	Art. 21(2)(g)	☐ Y ☐ P ☐ N
32	All staff receive security awareness training , including phishing.	Art. 21(2)(g)	☐ Y ☐ P ☐ N
33	A cryptography policy defines approved algorithms and the key lifecycle.	Art. 21(2)(h)	☐ Y ☐ P ☐ N
34	Data is encrypted in transit and at rest where appropriate.	Art. 21(2)(h)	☐ Y ☐ P ☐ N

35	Human resources security covers joiners, movers and leavers, confidentiality and lawful screening.	Art. 21(2)(i)	☐ Y ☐ P ☐ N
36	Access control follows least privilege, privileged access is managed, and rights are reviewed periodically.	Art. 21(2)(i)	☐ Y ☐ P ☐ N
37	An asset inventory of hardware, software, data and owners is kept current.	Art. 21(2)(i)	☐ Y ☐ P ☐ N
38	Multi-factor or continuous authentication protects remote, administrative and critical access.	Art. 21(2)(j)	☐ Y ☐ P ☐ N
39	Secured voice, video and text communications and a secured emergency communication system are in place where appropriate.	Art. 21(2)(j)	☐ Y ☐ P ☐ N
40	You have documented why your measures are proportionate to your exposure, size, and the likelihood and severity of incidents.	Art. 21(1)	☐ Y ☐ P ☐ N
41	If you are a DNS, TLD, cloud, data centre, CDN, MSP, MSSP, marketplace, search, social network or trust provider, your measures are mapped to Implementing Regulation (EU) 2024/2690 .	Art. 21(5); Reg. 2024/2690	☐ Y ☐ P ☐ N

4 • Incident reporting and supervision

#	CHECK	REFERENCE	STATUS
42	Your criteria for a significant incident are written down: severe disruption or financial loss, or considerable damage to others.	Art. 23(3); Reg. 2024/2690	☐ Y ☐ P ☐ N
43	A 24-hour early warning runbook says who decides, who sends it, to which CSIRT, and how it works out of hours.	Art. 23(4)(a)	☐ Y ☐ P ☐ N
44	You can produce a 72-hour incident notification with an initial assessment of severity, impact and indicators of compromise.	Art. 23(4)(b)	☐ Y ☐ P ☐ N
45	You can deliver a final report within one month (root cause, mitigation, cross-border impact), or a progress report if the incident is still ongoing.	Art. 23(4)(d)–(e)	☐ Y ☐ P ☐ N
46	You know how to notify recipients of your services about significant incidents and threats. A GDPR breach notice to the data protection authority (72h) runs in parallel.	Art. 23(1)–(2); GDPR Art. 33	☐ Y ☐ P ☐ N
47	An evidence pack is ready for the supervisor: documented policies, audit results and proof of implementation.	Art. 32(2)(e)–(g), 33(2)(d)–(f)	☐ Y ☐ P ☐ N

Your score

Count **2 points** for each Yes, **1** for each Partial and **0** for each No. Maximum: 94.

Score	Reading
80–94	Solid foundation. Focus on evidence quality and on testing your 24h / 72h reporting chain.
50–79	Real gaps. Prioritise governance (section 2) and reporting (section 4): they are usually the quickest to fix.
0–49	Start with scope, board approval and an incident runbook. A structured gap assessment is the next step.

These bands are an indicative prioritisation aid, not a compliance determination.

Want a second pair of eyes on your gaps?

Book a call and bring your score. We will look at your three weakest sections and what to fix first.

calendly.com/ansulev · info@ansulev.com · ansulev.com

Sources

Directive (EU) 2022/2555 (NIS2), OJ L 333, 27.12.2022 · Commission Implementing Regulation (EU) 2024/2690 · ENISA, *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0, June 2025 · Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (Ministerio del Interior, TRIS notification 26686) · European Commission, NIS2 infringement referral, 8 July 2026 · RD-ley 12/2018 and RD 43/2021.

Pending EU changes, not yet law on 2026-10-07: the Digital Omnibus (single incident-reporting entry point, proposed 19 November 2025) and targeted NIS2 amendments COM(2026) 13 (proposed 20 January 2026).

This checklist is general information, not legal advice. Your obligations depend on your sector, size, Member State and final national law.

© Angel Georgiev Sulev · All rights reserved